High Performance Network Security

FortiAnalyzer - CLI Reference

VERSION 5.0.13

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 14, 2016

FortiAnalyzer 5.0.13 CLI Reference

05-5013-185032-20160714

TABLE OF CONTENTS

Change Log **11**
Introduction **12**
FortiAnalyzerdocumentation 12
What's New in FortiAnalyzer 5.0 ..... **13**
FortiAnalyzer 5.0.13 13
FortiAnalyzer 5.0.11 13
FortiAnalyzer 5.0.10 13
FortiAnalyzer 5.0.9 14
FortiAnalyzer 5.0.8 15
FortiAnalyzer 5.0.7 16
FortiAnalyzer 5.0.6 19
FortiAnalyzer 5.0.5 20
FortiAnalyzer 5.0.4 24
Using the Command Line Interface **26**
CLI command syntax 26
Connecting to the CLI 27
Connecting to the FortiAnalyzer console 27
Setting administrative access on an interface 28
Connecting to the FortiAnalyzer CLI using SSH 28
Connecting to the FortiAnalyzer CLI using the GUI 29
CLI objects 29
CLI command branches 29
config branch 29
get branch 31
show branch 33
execute branch 34
diagnose branch 35
Example command sequences 35
CLI basics 36
Command help 36
Command tree 36
Command completion 36
Recalling commands 36
Editing commands 37

Line continuation 37
Command abbreviation 37
Environment variables 37
Encrypted password support 38
Entering spaces in strings 38
Entering quotation marks in strings 38
Entering a question mark (?) in a string 38
International characters 39
Special characters 39
IP address formats 39
Changing the baud rate 39
Debug log levels 39
Administrative Domains 41
About ADOMs 41
Configuring ADOMs 42
system 44
admin 44
admin group 44
admin ldap 45
admin profile 47
admin radius 48
admin setting 49
admin tacacs 51
admin user 52
aggregation-client 60
aggregation-service 63
alert-console 64
alert-event 65
alertemail 67
auto-delete 69
backup 70
backup all-settings 70
central-management 71
certificate 72
certificate ca 72
certificate crl 73
certificate local 74
certificate oftp 75
certificate ssh 75
dns 76
fips 77
global 77

interface 83
locallog 85
locallog disk setting 85
locallog filter 88
locallog fortianalyzer setting 90
locallog memory setting 91
locallog syslogd (syslogd2, syslogd3) setting 92
log 93
log alert 93
log fortianalyzer 94
log settings 95
mail 99
ntp 99
password-policy 100
report 101
report auto-cache 101
report est-browse-time 102
report group 103
report setting 103
route 104
route6 105
snmp 105
snmp community 105
snmp sysinfo 109
snmp user 110
sql 112
syslog 115
fmupdate 117
analyzer 117
analyzer virus report 117
av-ips 117
av-ips advanced-log 118
av-ips fct server-override 118
av-ips fgt server-override 119
av-ips push-override 120
av-ips push-override-to-client 121
av-ips update-schedule 121
av-ips web-proxy 122
device-version 123
disk-quota 124
fct-services 125
multilayer 125

publicnetwork 126
server-access-priorities 126
config private-server 127
server-override-status 127
service 128
support-pre-fgt43 128
execute 129
add-vm-license 129
backup 130
backup all-settings 130
backup logs 131
backup logs-only 131
backup logs-rescue 131
backup reports 132
backup reports-config 133
bootimage 133
certificate 134
certificate ca 134
certificate local 134
console 135
console baudrate 135
date 136
device 136
factory-license 137
fgfm 137
fgfm reclaim-dev-tunnel 137
fmupdate 137
format 138
log 139
log device disk_quota 139
log device logstore 140
log device permissions 140
log dlp-files 141
log import 141
log ips-pkt 142
log quarantine-files 142
log-aggregation 142
log-integrity 142
lvm 143
ping 143
ping6 144
raid 144

reboot 145
remove 145
reset 145
reset-sqllog-transfer 145
restore 146
restore all-settings 146
restore image 147
restore {logs | logs-only} 147
restore reports 148
restore reports-config 149
shutdown 149
sql-local 150
sql-local rebuild-db 150
sql-local remove-db 150
sql-local remove-logtype 150
sql-query-dataset 151
sql-query-generic 151
sql-report 152
ssh 153
ssh-known-hosts 153
time 154
top 154
traceroute 156
traceroute6 156
diagnose 157
auto-delete 157
cdb check 158
debug 158
debug application 158
debug cli 161
debug console 161
debug crashlog 162
debug disable 162
debug enable 162
debug info 162
debug reset 162
debug service 163
debug sysinfo 163
debug sysinfo-log 163
debug sysinfo-log-backup 163
debug sysinfo-log-list 164
debug timestamp 164

debug vminfo 164
dlp-archives 165
dlp-archives quar-cache 165
dlp-archives rebuild-quar-db 165
dlp-archives statistics 165
dlp-archives status 165
dvm 166
dvm adom 166
dvm chassis 166
dvm check-integrity 166
dvm debug 166
dvm device 167
dvm device-tree-update 167
dvm group 167
dvm lock 168
dvm proc 168
dvm task 168
dvm transaction-flag 169
fgfm 169
fmnetwork 169
fmnetwork arp 169
fmnetwork interface 170
fmnetwork netstat 170
fmupdate 170
fortilogd 173
hardware 174
log device 174
pm2 174
report 174
sniffer 175
sql 179
system 181
system admin-session 181
system disk 181
system export 182
system flash 183
system fsck 183
system geoip 184
system ntp 184
system print 184
system process 186
system raid 186

system route 186
system route6 187
test 187
test application 187
test connection 188
test sftp 188
upload 189
upload clear 189
upload force-retry 189
upload status 189
vpn 189
get 190
system admin 190
system aggregation-client 192
system aggregation-service 192
system alert-console 192
system alert-event 193
system alertemail 193
system auto-delete 193
system backup 194
system certificate 194
system dns 195
system fips 195
system global 195
system interface 196
system locallog 197
system log 197
system mail 198
system ntp 198
system password-policy 198
system performance 199
system report 199
system route 200
system route6 200
system snmp 200
system sql 201
system status 201
system syslog 201
show 202
Appendix A - Object Tables 203
Global object categories 203
Device object ID values 204

Appendix B - Maximum Values Table **208**
Maximum values tables 208
Appendix C - CLI Error Codes **211**

Change Log

Date	Change Description
2012-11-23	Initial release.
2013-01-11	Updated for FortiAnalyzer 5.0.1.
2013-03-28	Updated for FortiAnalyzer 5.0.2.
2013-04-26	The `execute lvm` command was added.
2013-07-16	Updated for FortiAnalyzer 5.0.3.
2013-09-13	Updated for FortiAnalyzer 5.0.4.
2013-11-12	Updated for FortiAnalyzer 5.0.5.
2014-02-05	Updated for FortiAnalyzer 5.0.6.
2014-07-02	Updated for FortiAnalyzer 5.0.7.
2014-07-11	Updated `config system snmp user` command information.
2014-10-07	Updated for FortiAnalyzer 5.0.8.
2014-10-17	Updated for FortiAnalyzer 5.0.9.
2014-12-04	Removed the `execute sql-local rebuild-device` and `execute sql-local remove-device` commands.
2014-12-18	Removed the `execute sql-local remove-log` command.
2015-02-06	Updated for FortiAnalyzer 5.0.10.
2015-06-16	Updated for FortiAnalyzer 5.0.11

Introduction

FortiAnalyzerplatforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

FortiAnalyzer offers enterprise class features to identify threats, while providing the flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements, while aggregating logs in a hierarchical, tiered logging topology.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

FortiAnalyzerdocumentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*
  This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *FortiAnalyzer device QuickStart Guides*
  These documents are included with your FortiAnalyzer system package. Use this document to install and begin working with the FortiAnalyzer system and FortiAnalyzer GUI.
- *FortiAnalyzer Online Help*
  You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the FortiAnalyzer GUI to configure and manage FortiGate units.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all FortiAnalyzer CLI commands.
- *FortiAnalyzer Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*
  This document describes installing FortiAnalyzer VM in your virtual environment.

What's New in FortiAnalyzer 5.0

FortiAnalyzer 5.0.13

No changes to the CLI have been made in FortiAnalyzer 5.0.13.

FortiAnalyzer 5.0.11

The table below list commands which have changed in 5.0.11.

Command	Change
`config system locallog ... filter`	Variable added: `devops`
`config system log settings`	Variable added: `sync-search-timeout`
`diagnose cdb check`	Variable added: `reference-integrity`

FortiAnalyzer 5.0.10

The table below list commands which have changed in 5.0.10.

Command	Change
`config system admin user > dashboard`	Variable added: `time-period`
`config system admin setting`	Variable added: `show-checkbox-in-table`
`config system log settings`	Variable added: `log-file-archive-name`

Command	Change

`config system sql`	Variables removed:
	`auto-table-upgrade`
	`table-partition-time-max`
	Variables added:
	`device-count-high`
	`traffic-table-partition-time`
	`event-table-partition-time`
	`utm-table-partition-time`

`config system report setting`	Variables added:
	`report-priority`
	`hcache-lossless`

`config system report group`	Command added.

`execute sql-report`	Variables added:
	`list`
	`view`
	`hcache-check`
	`list-schedule`
	Variable changed:
	`run`

`diagnose cdb check`	Variable added: `update-devinfo`
`diagnose sql status`	Variable added: `sql_hcache_chk`

FortiAnalyzer 5.0.9

The table below list commands which have changed in 5.0.9.

Command	Change
`config system global`	Variable added: `ssl-protocol`

FortiAnalyzer 5.0.8

The table below list commands which have changed in 5.0.8.

Command	Change
`config system global`	Variable added: `max-aggregation-tasks`
`config system admin profile`	Variable added: `change-password`
`config system admin user`	Variable added `change-password`

`config system admin settng`	Variables added:
	`admin-https-redirect`
	`show-log-forwarding`

`config system log settings`	Variable added: `FSA-custom-field1`

`config system aggregation-service`	Command added.
	Variables added:
	`accept-realtime-log`
	`accept-aggregation`
	`password`
	`aggregation-disk-quota`

`diagnose debug reset`	Command added.
`diagnose log array`	Command removed.

`diagnose sql config top-dev set`	Command added.
	Variables added:
	`log-thres`
	`num-max`

`execute devicelog clear`	Command removed.

`config system report auto-cache`	Variables added:
	`order`
	`aggressive-schedule`
	`drilldown-status`

Command	Change
`diagnose sql rebuild-report-hcache`	Command added.

`execute log device logstore`	Command added.
	Variables added:
	`list`
	`clear`
	`move`

FortiAnalyzer 5.0.7

The table below list commands which have changed in 5.0.7.

Command	Change

`config system admin ldap`	Variables added:
	`connect-timeout`
	`adom`

`config system auto-delete`	Command renamed: `regular-auto-deletion to log-auto-deletion`

`config system fips`	Variables added:
	`status`
	`fortitrng`
	`re-seed-interval`

`config system global`	Variable added:
	`tftp`
	`task-list-size`

`config system locallog [memory| disk | fortianalyzer | syslogd | syslogd2 | syslogd3] filter`	Variables added:
	`faz`
	`logd`
	`fips`

`config system localllog syslogd/syslogd2/syslogd3`	Variable added:
	`syslog-name`
	Variables removed:
	`server`
	`port`

Command	Change
`config system certificate`	Command added: `oftp`
`config system interface`	Variable removed: `serviceaccess`

`config system admin profile`	Variables removed:
	`type`
	`web-filter`
	`ips-filter`
	`app-filter`
	`global-policy-packages`
	`global-objects`
	`assignment`
	`read-passwd`
	`device-config`
	`device-profile`
	`policy-objects`
	`deploy-management`
	`config-retrieve`
	`term-access`
	`adom-policy-packages`
	`adom-policy-objects`
	`vpn-manager`
	`consistency-check`
	`faz-management`
	`fgd_center`
	`workflow-approve`
	`network`
	`admin`
	`system`
	`devices`
	`alerts`
	`dlp`
	`reports`
	`logs`
	`quar`
	`net-monitor`
	`vuln-mgmt`

`config system log settings`	Variables removed:
	`FGT-custom-field2 .. 5`
	`FCT-custom-field2 .. 5`
	`FML-custom-field2 .. 5`
	`FWB-custom-field2 .. 5`
	`FCH-custom-field2 .. 5`
	`FAZ-custom-field2 .. 5`

Command	Change

`config system sql`	Variables removed:
	`event-table-partition-time`
	`event-table-partition-time-max`
	`event-table-partition-time-min`
	`table-partition-mode`
	`traffic-table-partition-time`
	`traffic-table-partition-time-max`
	`traffic-table-partition-time-min`
	`utm-table-partition-time`
	`utm-table-partition-time-max`
	`utm-table-partition-time-min`

`diagnose report`	Command removed: `maintain`
`diagnose system server`	Command removed: `start`

`diagnose test`	Commands removed:
	`policy-check`
	`search`

`diagnose debug`	Commands added:
	`crashlog`
	`sysinfo-log`
	`sysinfo-log-backup`
	`sysinfo-log-list`
	Command removed:
	`dpm`

`diagnose debug application`	Command added: `dmworker`
`diagnose fortilogd`	Variable added: `lograte`

Command	Change

`diagnose pm2`	Commands added:
	`check-integrity`
	`print`

`execute remove reports`	Variable added: `<device-id>`

`execute sql-report`	Variables added:
	`list-lang`
	`import-lang`

FortiAnalyzer 5.0.6

The table below list commands which have changed in 5.0.6.

Command	Change
`config system admin ldap`	Variable added: `attributes`

`config system global`	Variable added:
	`webservice-proto`
	Variable removed:
	`webservice-support-sslv3`

`config system report setting`	Command added

`config system sql`	Variables added:
	`rebuild-event`
	`rebuils-event-start-time`

`config fmupdate device-version`	Variable added: `fsa`
`execute fmupdate cdrom`	Command removed
`execute log-aggregation`	Variable added: `<id>`
`execute raid`	Variable added: `rebuild-ecc`

Command	Change
`diagnose auto-delete`	Command added

`diagnose debug application`	Variable added:
	`ipsec`
	Variable removed:
	`ike`

`diagnose dvm device`	Variable added: `delete`
`diagnose log array`	Command added.
`diagnose sql remove`	Variable added: `query-cache`
`diagnose system raid`	Variable added: `alarms`
`diagnose test application`	Variable added: `fazautormd`
`diagnose vpn tunnel`	Command added

FortiAnalyzer 5.0.5

The table below list commands which have changed in 5.0.5.

Command	Change
`config system`	Variable added: `central-management`

`config system global`	Variables added:
	`search-all-adoms`
	`unregister-pop-up`

Command	Change

`config fmupdate`	Commands added:
	`analyzer`
	`av-ips`
	`device-version`
	`disk-quota`
	`fct-services`
	`fds-setting`
	`multilayer`
	`publicnetwork`
	`server-access-priorities`
	`server-override-status`
	`service`
	`support-pre-fgt43`

`execute backup`	Variable added: `logs-rescue`

Command	Change

`config systen admin setting`	Variables removed:
	`demo-mode`
	`device-sync status`
	`offline-mode`
	`allow_register`
	`register_passwd`
	`show_grouping_script`
	`show_automatic_script`
	`show_tcl_script`
	`auto-update`
	`mgmt-addr`
	`mgmt-fqdn`
	`show-global-policy-settings`
	`show-global-object-settings`
	`show-adom-ipv6-settings`
	`show-adom-dynamic-objects`
	`show-adom-dos-policies`
	`show-adom-sniffer-policies`
	`show-adom-central-nat-policies`
	`show-adom-voip-policies`
	`show-adom-icap-policies`
	`show-adom-implicit-policy`
	`show-adom-implicit-id-based-policy`
	`show-adom-taskmon-button`
	`show-adom-terminal-button`
	`show-adom-policy-consistency-button`
	`show-adom-rtmlog`
	`show-adom-vpnman`
	`show-adom-devman`
	`show-fortimail-settings`
	`show-foc-settings`
	`show-fsw-settings`
	`install-ifpolicy-only`

`config system log settings`	Variables added:
	`FAZ-custom-field1`
	`FAZ-custom-field2`
	`FAZ-custom-field3`
	`FAZ-custom-field4`
	`FAZ-custom-field5`

Command	Change

`config system aggregation-client`	Commands added:
	`server-device`
	`server-name`
	Sub-command added:
	`config device-filter`

`diagnose fmupdate`	Commands added:
	`add-device`
	`deldevice`
	`dellog`
	`fct-configure`
	`fct-dbcontract`
	`fct-delserverlist`
	`fct-getobject`
	`fct-serverlist`
	`fct-update-status`
	`fct-updatenow`
	`fds-configure`
	`fds-dbcontract`
	`fds-delserverlist`
	`fds-dump-breg`
	`fds-dump-srul`
	`fds-get-downstream-device`
	`fds-getobject`
	`fds-serverlist`
	`fds-service-info`
	`fds-update-status`
	`fds-updatenow`
	`fgd-updatenow`
	`fgt-del-statistics`
	`fgt-del-um-db`
	`fmg-statistic-info`
	`fortitoken`
	`getdevice`
	`service-restart`
	`show-bandwidth`
	`show-dev-obj`
	`view-linkd-log`
	`vm-license`

`execute fmupdate`	Commands added:
	`cdrom {import | list | mount | umount}`
	`ftp {export | import}`
	`scp {export | import}`
	`tftp {export | import}`

`diagnose fgfm`	Commands removed:
	`session-list`
	`install-sessions`

FortiAnalyzer 5.0.4

The table below list commands which have changed in 5.0.4.

Command	Change
`config system auto-delete`	New command added for automatic deletion policy for logs, reports, archived, and quarantined files.
`config system sql` `  config ts-index-field`	New sub-command added to configure SQL text search index fields.
`config system global` `  set backup-compression {high | low | none | normal}`	New set command added to set the compression level.
`config system global` `  set backup-to-subfolders {enable | disable}`	New set command added to enable or disable the creation of subfolders on server for backup storage.
`config system global` `  set lcdpin`	Legacy set command removed.
`config system global` `  set log-checksum {md5 | md5-auth | none}`	New set command added to record the log file hash value, timestamp, and authentication code at transmission or rolling.
`execute log-integrity`	New command added to query the log file's MD5 checksum and timestamp.
`execute log device permissions`	New command added to set log device permissions.
`execute log import`	New command added to allow import of logs and replace the log device ID.
`diagnose dvm supported-platforms list`	Command removed.
`diagnose sql show log-filters`	New command added to show log view searching filters.
`config system aggregation-client` `  set fwd-remote-server cef`	New variable added to allow logs to be forwarded to a CEF (Common Event Format) server.

Command	Change

`config system report auto-cache`
`set aggressive-drilldown`
`set drilldown-interval`
`set status`
	New command and variables added for report auto-cache settings.

`config system report est-browse time`
`set max-num-user`
`set status`
	New command and variables added for report estimated browse time settings.

`diagnose sql auto-hcache`	Command removed.

`config rolling-regular`
`set upload-mode backup`
`set ip2`
`set ip3`
`set username2`
`set username3`
`set password2`
`set password3`
	Added variables to allow up to three servers to be configured for log upload.

`diagnose report status`
`diagnose report clean`
`diagnose report maintain`
	Added new commands to cleanup, maintain, and get the status of the report queue.

`config rolling-analyzer` `config rolling-local`	Commands and related variables removed.

Using the Command Line Interface

This chapter explains how to connect to the Command Line Interface (CLI) and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

- CLI command syntax
- Connecting to the CLI
- CLI objects
- CLI command branches
- CLI basics

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets `<  >` indicate variables.
- Vertical bar and curly brackets `{ | }` separate alternative, mutually exclusive required variables.

  For example:

  ```
  set protocol {ftp | sftp}
  ```

  You can enter `set protocol ftp` or `set protocol sftp`.

- Square brackets `[  ]` indicate that a variable is optional.

  For example:

  ```
  show system interface [<name_str>]
  ```

  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.

- A space separates options that can be entered in any combination and must be separated by spaces.

  For example:

  ```
  set allowaccess {https ping ssh snmp telnet http webservice aggregator}
  ```

  You can enter any of the following:

  ```
  set allowaccess ping
  set allowaccess https
  set allowaccess ssh
  set allowaccess https ssh
  set allowaccess aggregator http https ping ssh telnet webservice
  ```

  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

- Special characters:
  - The \ is supported to escape spaces or as a line continuation character.
  - The single quotation mark ' and the double quotation mark “ are supported, but must be used in pairs.

- If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Connecting to the CLI

You can use a direct console connection or SSH to connect to the FortiAnalyzer CLI. You can also access through the CLI console widget on the GUI. For more information, see the *FortiAnalyzer Administration Guide*, and your device's QuickStart Guide.

You can use a direct console connection or SSH to connect to the FortiAnalyzer CLI.

Connecting to the FortiAnalyzer console

To connect to the FortiAnalyzer console, you need:

- a computer with an available communications port
- a console cable, provided with your FortiAnalyzer unit, to connect the FortiAnalyzer console port and a communications port on your computer
- terminal emulation software, such as HyperTerminal for Windows.

The following procedure describes how to connect to the FortiAnalyzer CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

1. Connect the FortiAnalyzer console port to the available communications port on your computer.
2. Make sure the FortiAnalyzer unit is powered on.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the FortiAnalyzer console port.
5. Select *OK*.
6. Select the following port settings and select *OK*.

COM port	COM1
Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press `Enter` to connect to the FortiAnalyzer CLI. A login prompt appears.
8. Type a valid administrator name and press `Enter`.
9. Type the password for this administrator and press `Enter`. A command prompt appears.

You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Setting administrative access on an interface

To perform administrative functions through a FortiAnalyzer network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the GUI to configure FortiAnalyzer interfaces for SSH access, see the *FortiAnalyzer Administration Guide*.

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiAnalyzer console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:
```
config system interface
   edit <interface_name>
      set allowaccess <access_types>
   end
```
Where `<interface_name>` is the name of the FortiAnalyzer interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.

For example, to configure port1 to accept HTTPS and SSH connections, enter:
```
config system interface
   edit port1
      set allowaccess https ssh
   end
```

Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiAnalyzer configuration.

3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:
```
get system interface <interface_name>
```
The CLI displays the settings, including the management access settings, for the named interface.

Connecting to the FortiAnalyzer CLI using SSH

SSH provides strong secure authentication and secure communications to the FortiAnalyzer CLI from your internal network or the internet. Once the FortiAnalyzer unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiAnalyzer CLI.

To connect to the CLI using SSH:

1. Install and start an SSH client.
2. Connect to a FortiAnalyzer interface that is configured for SSH connections.
3. Type a valid administrator name and press `Enter`.
4. Type the password for this administrator and press `Enter`.

The FortiAnalyzer model name followed by a # is displayed.

You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Connecting to the FortiAnalyzer CLI using the GUI

The GUI also provides a CLI console window.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
2. Go to *System Settings* > *Dashboard*
3. Click inside the CLI Console widget. If the widget is not available, select *Add Widget* to add the widget to the dashboard.

CLI objects

The FortiAnalyzer CLI is based on configurable objects. The top-level object are the basic components of FortiAnalyzer functionality.

system	Configuration options related to the overall operation of the FortiAnalyzer unit, such as interfaces, virtual domains, and administrators.
fmupdate	Configures settings related to FortiGuard service updates and the unit's built-in FDS.

This object contains more specific lower level objects. For example, the system object contains objects for administrators, DNS, interfaces and so on.

CLI command branches

The FortiAnalyzer CLI consists of the following command branches:

config branch	execute branch
get branch	diagnose branch
show branch	

Examples showing how to enter command sequences within each branch are provided in the following sections.

config branch

The `config` commands configure objects of FortiAnalyzer functionality. Top-level objects are not configurable, they are containers for more specific lower level objects. For example, the system object contains administrators, DNS addresses, interfaces, routes, and so on. When these objects have multiple sub-objects, such as administrators or routes, they are organized in the form of a table. You can add, delete, or edit the entries in the

table. Table entries each consist of variables that you can set to particular values. Simpler objects, such as system DNS, are a single set of variables.

To configure an object, you use the `config` command to navigate to the object's command "shell". For example, to configure administrators, you enter the command

```
config system admin user
```

The command prompt changes to show that you are in the admin shell.

```
(user)#
```

This is a table shell. You can use any of the following commands:

edit	Add an entry to the FortiAnalyzer configuration or edit an existing entry. For example in the `config system admin` shell: • Type `edit admin` and press `Enter` to edit the settings for the default admin administrator account. • Type `edit newadmin` and press `Enter` to create a new administrator account with the name `newadmin` and to edit the default settings for the new administrator account.
delete	Remove an entry from the FortiAnalyzer configuration. For example in the `config system admin` shell, type `delete newadmin` and press `Enter` to delete the administrator account named `newadmin`.
purge	Remove all entries configured in the current shell. For example in the `config user local` shell: • Type `get` to see the list of user names added to the FortiAnalyzer configuration, • Type `purge` and then `y` to confirm that you want to purge all the user names, • Type `get` again to confirm that no user names are displayed.
get	List the configuration. In a table shell, `get` lists the table members. In an edit shell, `get` lists the variables and their values.
show	Show changes to the default configuration as configuration commands.
end	Save the changes you have made in the current shell and leave the shell. Every `config` command must be paired with an `end` command. You will return to the root FortiAnalyzer CLI prompt. The `end` command is also used to save `set` command changes and leave the shell.

If you enter the `get` command, you see a list of the entries in the table of administrators. To add a new administrator, you enter the edit command with a new administrator name:

```
edit admin_1
```

The FortiAnalyzer unit acknowledges the new table entry and changes the command prompt to show that you are now editing the new entry:

```
new entry 'admin_1' added
(admin_1)#
```

From this prompt, you can use any of the following commands:

config	In a few cases, there are subcommands that you access using a second config command while editing a table entry. An example of this is the command to add restrict the user to specific devices or VDOMs.
set	Assign values. For example from the `edit admin` command shell, typing `set password newpass` changes the password of the admin administrator account to `newpass`. When using a set command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
unset	Reset values to defaults. For example from the `edit admin` command shell, typing `unset password` resets the password of the admin administrator account to the default of no password.
get	List the configuration. In a table shell, `get` lists the table members. In an edit shell, `get` lists the variables and their values.
show	Show changes to the default configuration in the form of configuration commands.
next	Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the `config system admin user` shell. • Type `edit User1` and press `Enter`. • Use the `set` commands to configure the values for the new admin account. • Type `next` to save the configuration for User1 without leaving the `config system admin user` shell. • Continue using the `edit`, `set`, and `next` commands to continue adding admin user accounts. • Type `end` and press `Enter` to save the last configuration and leave the shell.
abort	Exit an edit shell without saving the configuration.
end	Save the changes you have made in the current shell and leave the shell. Every `config` command must be paired with an `end` command. The `end` command is also used to save `set` command changes and leave the shell.

The `config` branch is organized into configuration shells. You can complete and save the configuration within each shell for that shell, or you can leave the shell without saving the configuration. You can only use the configuration commands for the shell that you are working in. To use the configuration commands for another shell you must leave the shell you are working in and enter the other shell.

get branch

Use `get` to display settings. You can use `get` within a `config` shell to display the settings for that shell, or you can use `get` with a full path to display the settings for the specified shell.

To use `get` from the root prompt, you must include a path to a shell.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `get` in the `config system admin user` shell, the list of administrators is displayed.

At the `(user)#` prompt, type:

```
get
```

The screen displays:

```
== [ admin ]
userid: admin
== [ admin2 ]
userid: admin2
== [ admin3 ]
userid: admin3
```

Example 2

When you type `get` in the `admin` user shell, the configuration values for the admin administrator account are displayed.

```
edit admin
```

At the `(admin)#` prompt, type:

```
get
```

The screen displays:

```
   userid : admin
   password : *
   trusthost1 : 0.0.0.0 0.0.0.0
   trusthost2 : 0.0.0.0 0.0.0.0
   trusthost3 : 0.0.0.0 0.0.0.0
   trusthost4 : 0.0.0.0 0.0.0.0
   trusthost5 : 0.0.0.0 0.0.0.0
   trusthost6 : 0.0.0.0 0.0.0.0
   trusthost7 : 0.0.0.0 0.0.0.0
   trusthost8 : 0.0.0.0 0.0.0.0
   trusthost9 : 0.0.0.0 0.0.0.0
   trusthost10 : 127.0.0.1 255.255.255.255
   ipv6_trusthost1 : ::/0
   ipv6_trusthost2 : ::/0
   ipv6_trusthost3 : ::/0
   ipv6_trusthost4 : ::/0
   ipv6_trusthost5 : ::/0
   ipv6_trusthost6 : ::/0
   ipv6_trusthost7 : ::/0
   ipv6_trusthost8 : ::/0
   ipv6_trusthost9 : ::/0
   ipv6_trusthost10 : ::1/128
   profileid : Super_User
   adom:
      == [ all_adoms ]
      adom-name: all_adoms
   policy-package:
      == [ all_policy_packages ]
      policy-package-name: all_policy_packages
   restrict-access : disable
   restrict-dev-vdom:
   description : (null)
```

```
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
meta-data:
last-name : (null)
first-name : (null)
email-address : (null)
phone-number : (null)
mobile-number : (null)
pager-number : (null)
hidden : 0
dashboard-tabs:
dashboard:
   == [ 6 ]
   moduleid: 6
   == [ 1 ]
   moduleid: 1
   == [ 2 ]
   moduleid: 2
   == [ 3 ]
   moduleid: 3
   == [ 4 ]
   moduleid: 4
   == [ 5 ]
   moduleid: 5
```

Example 3

You want to confirm the IP address and netmask of the port1 interface from the root prompt.

At the (command) # prompt, type:

```
get system interface port1
```

The screen displays:

```
name : port1
status : up
ip : 172.16.81.30 255.255.255.0
allowaccess : ping https ssh snmp telnet http webservice aggregator
serviceaccess :
speed : auto
description : (null)
alias : (null)
ipv6:
   ip6-address: ::/0 ip6-allowaccess:
```

show branch

Use `show` to display the FortiAnalyzer unit configuration. Only changes to the default configuration are displayed. You can use `show` within a `config` shell to display the configuration of that shell, or you can use `show` with a full path to display the configuration of the specified shell.

To display the configuration of all `config` shells, you can use `show` from the root prompt. The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `show` and press `Enter` within the `port1` interface shell, the changes to the default interface configuration are displayed.

At the `(port1)#` prompt, type:

```
show
```

The screen displays:

```
config system interface
   edit "port1"
      set ip 172.16.81.30 255.255.255.0
      set allowaccess ping https ssh snmp telnet http webservice aggregator
   next
   edit "port2"
      set ip 1.1.1.1 255.255.255.0
      set allowaccess ping https ssh snmp telnet http webservice aggregator
   next
   edit "port3"
   next
   edit "port4"
   next
end
```

Example 2

You are working in the `port1` interface shell and want to see the `system dns` configuration. At the `(port1)#` prompt, type:

```
show system dns
```

The screen displays:

```
config system dns
   set primary 65.39.139.53
   set secondary 65.39.139.63
end
```

execute branch

Use `execute` to run static commands, to reset the FortiAnalyzer unit to factory defaults, or to back up or restore the FortiAnalyzer configuration. The execute commands are available only from the root prompt.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example

At the root prompt, type:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

and press `Enter` to restart the FortiAnalyzer unit.

diagnose branch

Commands in the `diagnose` branch are used for debugging the operation of the FortiAnalyzer unit and to set parameters for displaying different levels of diagnostic information.

Diagnose commands are intended for advanced users only. Contact Fortinet Technical Support before using these commands.

Example command sequences

The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:
   ```
   config system dns
   ```
   and press `Enter`. The prompt changes to `(dns)#`.
2. At the `(dns)#` prompt, type (question mark) `?`
   The following options are displayed.
   ```
   set
   unset
   get
   show
   abort
   end
   ```
3. Type `set ?`
   The following options are displayed:
   ```
   primary
   secondary
   ```
4. To set the primary DNS server address to `172.16.100.100`, type:
   ```
   set primary 172.16.100.100
   ```
   and press `Enter`.
5. To set the secondary DNS server address to `207.104.200.1`, type:
   ```
   set secondary 207.104.200.1
   ```
   and press `Enter`.
6. To restore the primary DNS server address to the default address, type `unset primary` and press `Enter`.
7. If you want to leave the `config system dns` shell without saving your changes, type `abort` and press `Enter`.
8. To save your changes and exit the `dns` sub-shell, type `end` and press `Enter`.
9. To confirm your changes have taken effect after leaving the `dns` sub-shell, type `get system dns` and press `Enter`.

CLI basics

Command help

You can press the question mark (?) key to display command help.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Type a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.

Command tree

Type `tree` to display the FortiAnalyzer CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file. For `config` commands, use the `tree` command to view all available variables and sub-commands.

Example

```
#config system interface
(interface)# tree
-- [interface] --*name
              |- status
              |- ip
              |- allowaccess
              |- serviceaccess
              |- speed
              |- description
              |- alias
              +- <ipv6> -- ip6-address
                 +- ip6-allowaccess
```

Command completion

You can use the tab key or the question mark (?) key to complete commands:

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the left and right arrow keys to move the cursor back and forth in a recalled command. You can also use the backspace and delete keys and the control keys listed in the following table to edit the command.

Function	Key combination
Beginning of line	Control key + A
End of line	Control key + E
Back one character	Control key + B
Forward one character	Control key + F
Delete current character	Control key + D
Previous command	Control key + P
Next command	Control key + N
Abort the command	Control key + C
If used at the root prompt, exit the CLI	Control key + C

Line continuation

To break a long command over multiple lines, use a \ at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of unambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

Environment variables

The FortiAnalyzer CLI supports several environment variables.

$USERFROM	The management access type (SSH, Telnet and so on) and the IP address of the logged in administrator.
$USERNAME	The user account name of the logged in administrator.
$SerialNum	The serial number of the FortiAnalyzer unit.

Variable names are case sensitive. In the following example, when entering the variable, you can type (dollar sign) `$` followed by a tab to auto-complete the variable to ensure that you have the exact spelling and case. Continue pressing tab until the variable you want to use is displayed.

```
config system global
```

```
      set hostname $SerialNum
   end
```

Encrypted password support

After you enter a clear text password using the CLI, the FortiAnalyzer unit encrypts the password and stores it in the configuration file with the prefix ENC. For example:

```
show system admin user user1
config system admin user
   edit "user1"
      set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1
          rVJmMFc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9XqOit82PgScwzGzGuJ5a9
          f
      set profileid "Standard_User"
   next
end
```

It is also possible to enter an already encrypted password. For example, type:

```
config system admin
```

then press `Enter`.

Type:

```
edit user1
```

then press `Enter`.

Type:

```
set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMF
    c9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9XqOit82PgScwzGzGuJ5a9f
```

then press `Enter`.

Type:

```
end
```

then press `Enter`.

Entering spaces in strings

When a string value contains a space, do one of the following:

- Enclose the string in quotation marks, for example `"Security Administrator"`.
- Enclose the string in single quotes, for example `'Security Administrator'`.
- Use a backslash (“\”) preceding the space, for example `Security\ Administrator`.

Entering quotation marks in strings

If you want to include a quotation mark, single quote or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with CTRL-V. Entering a question mark without first entering CTRL-V causes the CLI to display possible command completions,

terminating the string.

International characters

The CLI supports international characters in strings.

Special characters

The characters <, >, (,), #, ’, and " are not permitted in most CLI fields, but you can use them in passwords. If you use the apostrophe (‘) or quote (") character, you must precede it with a backslash (\) character when entering it in the CLI `set` command.

IP address formats

You can enter an IP address and subnet using either dotted decimal or slash-bit format. For example you can type one of:

```
set ip 192.168.1.1 255.255.255.0
set ip 192.168.1.1/24
```

The IP address is displayed in the configuration file in dotted decimal format.

Changing the baud rate

Using `execute console baudrate`, you can change the default console connection baud rate.

To check the current baud rate enter the following CLI command:

```
# execute console baudrate [enter]
current baud rate is: 9600
```

To view baudrate options, enter the CLI command with the question mark (?).

```
# execute console baudrate ?
baudrate 9600 | 19200 | 38400 | 57600 | 115200
```

To change the baudrate, enter the CLI command as listed below.

```
# execute console baudrate 19200
Your console connection will get lost after changing baud rate.
Change your console setting!
Do you want to continue? (y/n)
```

Changing the default baud rate is not available on all models.

Debug log levels

The following table lists available debug log levels on your FortiAnalyzer .

Level	Type	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An erroneous condition exists and functionality is probably affected.
4	Warning	Function might be affected.
5	Notice	Notification of normal events.
6	Information	General information about system operations.
7	Debug	Detailed information useful for debugging purposes.
8	Maximum	Maximum log level.

Administrative Domains

Administrative domains (ADOMs) enable the admin administrator to constrain other Fortinet unit administrators' access privileges to a subset of devices in the device list. For FortiGate devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific FortiGate VDOM.

About ADOMs

Enabling ADOMs alters the structure and available functionality of the GUI and CLI according to whether you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile.

The `admin` administrator can further restrict other administrators' access to specific configuration areas within their ADOM by using access profiles .

Characteristics of the CLI and GUI when ADOMs are enabled

	admin administrator account	Other administrators
Access to config system global	Yes	No
Can create administrator accounts	Yes	No
Can enter all ADOMs	Yes	No

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.

  `config system global` contains settings used by the FortiAnalyzer unit itself and settings shared by ADOMs, such as the device list, RAID, and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.

- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, quarantine files, content archives, IP aliases, and LDAP queries specific to your ADOM. You cannot access Global Configuration, or enter other ADOMs.

  By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiAnalyzer unit's total devices or VDOMs.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or Global Configuration.

The maximum number of ADOMs varies by FortiAnalyzer model.

FortiAnalyzer Model	Maximum ADOMs
FAZ-100C	100
FAZ-200D	150
FAZ-300D	175
FAZ-400C	300
FAZ-1000C, and FAZ-1000D	2 000
FAZ-3000D and FAZ-3000E	2 000
FAZ-3500E and FAZ-3900E	4 000
FAZ-4000B	2 000
FAZ-VM32 and FAZ-VM64	10 000

Configuring ADOMs

To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign existing FortiAnalyzer administrators to ADOMs.

Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiAnalyzer unit configuration before enabling ADOMs.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the GUI.

To enable or disable ADOMs:

Enter the following CLI command:

```
config system global
   set adom-status {enable | disable}
end
```

An administrative domain has two modes: normal and advanced. Normal mode is the default device mode. In normal mode, a FortiGate unit can only be added to a single administrative domain. In advanced mode, you can assign different VDOMs from the same FortiGate to multiple administrative domains.

Enabling the advanced mode option will result in a reduced operation mode and more complicated management scenarios. It is recommended only for advanced users.

To change ADOM device modes:

Enter the following CLI command:

```
config system global
   set adom-mode {advanced | normal}
end
```

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
   edit <name>
      set adom <adom_name>
   next
end
```

where `<name>` is the administrator user name and `<adom_name>` is the ADOM name.

system

Use `system` commands to configure options related to the operation of the FortiAnalyzer unit.

FortiAnalyzer CLI commands and variables are case sensitive.

This chapter contains following sections:

admin	certificate	password-policy
aggregation-client	dns	report
aggregation-service	fips	route
alert-console	global	route6
alert-event	interface	snmp
alertemail	locallog	sql
auto-delete	log	syslog
backup	mail	
central-management	ntp	

For more information about configuring ADOMs, see Administrative Domains on page 41.

admin

Use the following commands to configure admin related settings:

admin group	admin setting
admin ldap	admin tacacs
admin profile	admin user
admin radius	

admin group

Use this command to add, edit, and delete admin user groups.

Syntax

```
config system admin group
   edit <group_name>
```

```
        set member <group_member_name_string>
    end
```

Variable	Description
`<group_name>`	Enter the name of the admin group you want to edit. Enter a new name to create a new entry.
`member <group_member_name_string>`	Enter the name of the member to add to this group. You can add multiple members to the group. Enter question mark (`?`) to view available members.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin group
```

admin ldap

Use this command to add, edit, and delete Lightweight Directory Access Protocol (LDAP) users.

Syntax

```
config system admin ldap
   edit <LDAP server entry>
      set attributes <filter>
      set server {name_string | ip_string}
      set cnid <string>
      set dn <string>
      set port <integer>
      set type {anonymous | regular | simple}
      set username <string>
      set password <string>
      set group <string>
      set filter <query_string>
      set secure {disable | ldaps | starttls}
      set ca-cert <string>
      set connect-timeout <integer>
      set adom <adom-name>
end
```

Variable	Description	Default
`<LDAP server entry>`	Enter the name of the LDAP server you want to edit. Enter a new name to create a new entry.	
`attributes <filter>`	Attributes used for group searching, such as `member`, or `uniquemember`. Multiple attributes can be added when separated by a comma.	
`server {name_string | ip_string}`	Enter the LDAP server domain name or IPv4 address.	
`cnid <string>`	Enter common name identifier.	cn

Variable	Description	Default
`dn <string>`	Enter the distinguished name.	
`port <integer>`	Enter the port number for LDAP server communication.	389
`type {anonymous | regular | simple}`	Set a binding type: • `anonymous`: Bind using anonymous user search. • `regular`: Bind using username or password and then search. • `simple`: Simple password authentication without search.	simple
`username <string>`	Enter a username. This variable appears only when `type` is set to `regular`.	
`password <string>`	Enter a password for the username above. This variable appears only when `type` is set to `regular`.	
`group <string>`	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.	
`filter <query_string>`	Enter content for group searching. For example: • `(&(objectcategory=group)(member=*))` • `(&(objectclass=groupofnames)(member=*))` • `(&(objectclass=groupofuniquenames)(uniquemember=*))` • `(&(objectclass=posixgroup)(memberuid=*))`	
`secure {disable | ldaps | starttls}`	Set the SSL connection type: • `disable`: No SSL connection required • `ldaps`: Use LDAP over SSL • `starttls`: Use STARTTLS	disable
`ca-cert <string>`	CA certificate name. This variable appears only when `secure` is set to `ldaps` or `starttls`.	500
`connect-timeout <integer>`	Set the LDAP connection timeout (msec).	
`adom <adom-name>`	Set the ADOM to associate with the LDAP configuration.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin ldap
```

admin profile

Use this command to configure access profiles. In a newly-created access profile, no access is enabled.

Syntax

```
config system admin profile
   edit <profile_name>
      set description <text>
      set scope {adom | global}
      set system-setting {none | read | read-write}
      set adom-switch {none | read | read-write}
      set device-manager {none | read | read-write}
      set device-op {none | read | read-write}
      set realtime-monitor {none | read | read-write}
      set log-viewer {none | read | read-write}
      set report-viewer {none | read | read-write}
      set event-management {none | read | read-write}
      set change-password {enable | disable}>
   end
```

Variable	Description	Default
`<profile_name>`	Edit the access profile. Enter a new name to create a new profile. The pre-defined access profiles are: • `Super_User`: Super user profiles have all system and device privileges enabled. • `Standard_User`: Standard user profiles have no system privileges enabled, but have read/write access for all device privileges. • `Restricted_User`: Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.	
`description <text>`	Enter a description for this access profile. Enclose the description in quotes if it contains spaces.	
`scope {adom | global}`	Set the scope for this access profile to either ADOM or Global.	global
`system-setting {none | read | read-write}`	Configure System Settings permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`adom-switch {none | read | read-write}`	Configure administrator domain (ADOM) permissions for this profile.	none

Variable	Description	Default
`device-manager {none | read | read-write}`	Configure Device Manager permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`device-op {none | read | read-write}`	Add the capability to add, delete, and edit devices to this profile.	none
`realtime-monitor {none | read | read-write}`	Configure Drill Down configuration permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`log-viewer {none | read | read-write}`	Configure Log View permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`report-viewer {none | read | read-write}`	Configure Reports permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`event-management {none | read | read-write}`	Configure Event Management permissions for this profile. Select `none` to hide this option from the administrator in the GUI.	none
`change-password {enable | disable}`	Enable/disable restricted user to change self password.	disable

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin profile
```

admin radius

Use this command to add, edit, and delete administration RADIUS servers.

Syntax

```
config system admin radius
   edit <server_name>
      set auth-type <auth_prot_type>
      set nas-ip <ipv4_address>
      set port <integer>
      set secondary-secret <password>
      set secondary-server <string>
      set secret <password>
      set server <string>
end
```

Variable	Description	Default
`<server_name>`	Enter the name of the server you want to edit. Enter a new name to create a new entry.	
`auth-type <auth_prot_type>`	Enter the authentication protocol the RADIUS server will use: • `any`: Use any supported authentication protocol. • `mschap2`: MSCHAPv2 • `chap`: CHAP • `pap`: PAP	any
`nas-ip <ipv4_address>`	Enter the NAS IPv4 address.	0.0.0.0
`port <integer>`	Enter the RADIUS server port number.	1812
`secondary-secret <password>`	Enter the server secret (password) to access the RADIUS secondary-server.	
`secondary-server <string>`	Enter the RADIUS secondary-server DNS resolvable domain name or IPv4 address.	
`secret <password>`	Enter the server secret (password) to access the RADIUS server.	
`server <string>`	Enter the RADIUS server DNS resolvable domain name or IPv4 address.	

Use the `show` command to display the current configuration:

```
show system admin radius
```

admin setting

Use this command to configure system administration settings, including web administration ports, timeout, and language.

Syntax

```
config system admin setting
   set access-banner {enable | disable}
   set admin-https-redirect {enable | disable}
   set admin_server_cert <admin_server_certificate>
   set banner-message <string>
   set http_port <integer>
   set https_port <integer>
   set idle_timeout <integer>
   set show-add-multiple {enable | disable}
   set show-checkbox-in-table {enable | disable}
   set show-device-import-export {enable | disable}
   set show-log-forwarding {enable | disable}
   set unreg_dev_opt {add_allow_service | add_no_service}
```

```
    set webadmin_language {auto_detect | english | japanese | korean | simplified_
        chinese | traditional_chinese}
end
```

Variable	Description	Default
`access-banner {enable | disable}`	Enable/disable the access banner.	disable
`admin-https-redirect {enable | disable}`	Enable/disable redirection of HTTP admin traffic to HTTPS.	enable
`admin_server_cert <admin_server_certificate>`	Enter the name of an HTTPS server certificate to use for secure connections. FortiAnalyzer has the following certificates pre-loaded: • server.crt • Fortinet_Local	server.crt
`banner-message <string>`	Enter a banner message. Maximum of 255 characters.	
`http_port <integer>`	Enter the HTTP port number for web administration.	80
`https_port <integer>`	Enter the HTTPS port number for web administration.	443
`idle_timeout <integer>`	Enter the idle timeout value. The range is from 1 to 480 minutes.	5
`show-add-multiple {enable | disable}`	Enable/disable show the add multiple button in the GUI.	
`show-checkbox-in-table {enable | disable}`	Show checkboxes in tables in the GUI.	
`show-device-import-export {enable | disable}`	Enable/disable import/export of ADOM, device, and group lists.	
`show-log-forwarding {enable | disable}`	Enable/disable show log forwarding tab in Analyzer mode.	

Variable	Description	Default
`unreg_dev_opt {add_allow_service | add_no_service}`	Select action to take when an unregistered device connects to FortiAnalyzer. • `add_allow_service`: Add unregistered devices and allow service requests. • `add_no_service`: Add unregistered devices and deny service requests.	add_allow_services
`webadmin_language {auto_detect | english | japanese | korean | simplified_chinese | traditional_chinese}`	Enter the language to be used for web administration.	auto_detect

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin setting
```

admin tacacs

Use this command to add, edit, and delete administration TACACS+ servers.

Syntax

```
config system admin tacacs
   edit <name_string>
      set authen-type <auth_prot_type>
      set authorization {enable | disable}
      set key <password>
      set port <integer>
      set secondary-key <password>
      set secondary-server <string>
      set server <string>
      set tertiary-key <password>
      set tertiary-server <string>
end
```

Variable	Description	Default
`<name_string>`	Enter the name of the TACACS+ server that you want to edit. Enter a new name to create a new entry.	

Variable	Description	Default
`authen-type <auth_prot_type>`	Choose which authentication type to use. Select one of the following: • `ascii`: ASCII • `auto`: Use PAP, MSCHAP, and CHAP (in this order) • `chap`: CHAP • `mschap`: MSCHAP • `pap`: PAP	auto
`authorization {enable | disable}`	Enable/disable TACACS+ authorization.	
`key <password>`	Key (password) to access the server.	
`port <integer>`	Port number of the TACACS+ server.	
`secondary-key <password>`	Key (password) to access the secondary server.	
`secondary-server <string>`	Secondary server domain name or IPv4 address.	
`server <string>`	The server domain name or IPv4 address.	
`tertiary-key <password>`	Key (password) to access the tertiary server.	
`tertiary-server <string>`	Tertiary server domain name or IPv4 address.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin tacacs
```

Example

This example shows how to add the TACACS+ server `TAC1` at the IPv4 address `206.205.204.203` and set the key as `R1a2D3i4U5s`.

```
config system admin tacacs
   edit TAC1
      set server 206.205.204.203
      set key R1a2D3i4U5s
   end
```

admin user

Use this command to add, edit, and delete administrator accounts.

Use the admin account or an account with System Settings read and write privileges to add new administrator accounts and control their permission levels. Each administrator account must include a minimum of an access

profile. The access profile list is ordered alphabetically, capitals first. If custom profiles are defined, it may change the default profile from Restricted_User. You cannot delete the admin administrator account. You cannot delete an administrator account if that user is logged on. For information about ADOMs, see Administrative Domains on page 41.

You can create meta-data fields for administrator accounts. These objects must be created using the FortiAnalyzer GUI. The only information you can add to the object is the value of the field (pre-determined text/numbers).

Syntax

```
config system admin user
   edit <name_string>
      set password <password>
      set change-password {enable | disable}
      set trusthost1 <ipv4_mask>
      set trusthost2 <ipv4_mask>
      set trusthost3 <ipv4_mask>
      ...
      set trusthost10 <ipv4_mask>
      set ipv6_trusthost1 <ipv6 prefix>
      set ipv6_trusthost2 <ipv6 prefix>
      set ipv6_trusthost3 <ipv6 prefix>
      ...
      set ipv6_trusthost10 <ipv6 prefix>
      set profileid <profile-name>
      set adom <adom_name(s)>
      set policy-package {<adom name>: <policy package id> <adom policy folder name>/
          <package name> | all_policy_packages}
      set restrict-access {enable | disable}
      set description <string>
      set user_type {group | local | pki-auth | radius | ldap | tacacs-plus}
      set ldap-server <string>
      set radius_server <string>
      set tacacs-plus-server <string>
      set group <group_name>
      set ssh-public-key1 <key-type> <key-value>
      set ssh-public-key2 <key-type>, <key-value>
      set ssh-public-key3 <key-type> <key-value>
      set wildcard {enable | disable}
      set radius-accprofile-override {enable | disable}
      set radius-adom-override {enable | disable}
      set radius-group-match <string>
      set password-expire <yyyy-mm-dd>
      set force-password-change {enable | disable}
      set subject <string>
      set ca <string>
      set two-factor-auth {enable | disable}
      set last-name <string>
      set first-name <string>
      set email-address <string>
      set phone-number <string>
      set mobile-number <string>
      set pager-number <string>
   end
   config meta-data
```

```
            edit fieldname
               set fieldlength
               set fieldvalue <string>
               set importance
               set status
            end
         end
         config dashboard-tabs
            edit tabid <integer>
               set name <string>
            end
         config dashboard
            edit moduleid
               set name <string>
               set column <column_pos>
               set refresh-inverval <integer>
               set status {close | open}
               set tabid <integer>
               set widget-type {alert | devsummary | jsconsole | licinfo | logrecv | raid |
                   rpteng | statisctics | sysinfo | sysop | sysres | top-lograte}
               set log-rate-type {device | log}
               set log-rate-topn {1 | 2 | 3 | 4 | 5}
               set log-rate-period {1hour | 2min | 6hours}
               set res-view-type {history | real-time}
               set res-period {10min | day | hour}
               set num-entries <integer>
               set res-cpu-display {average | each}
               set time-period {1hour | 24hour | 8hour}
            end
         end
         config restrict-dev-vdom
            edit dev-vdom <string>
         end
      end
```

Variable	Description	Default
`<name_string>`	Enter the name of the administrator user you want to edit. Enter a new name to create a new entry.	
`password <password>`	Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. This variable is available only if `user_type` is `local`.	
`change-password {enable | disable}`	Enable/disable restricted profile user to change self password.	

Variable	Description	Default

`trusthost1 <ipv4_mask>`
`trusthost2 <ipv4_mask>`
`trusthost3 <ipv4_mask>`
`...`
`trusthost10 <ipv4_mask>`
	Optionally, type the trusted host IPv4 address and netmask from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts (optional).
	Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 59.	

`ipv6_trusthost1 <ipv6 prefix>`
`ipv6_trusthost2 <ipv6 prefix>`
`...`
`ipv6_trusthost10 <ipv6 prefix>`
	Type the trusted host IPv6 address from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts. (optional).
	Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 59.	

`profileid <profile-name>`	Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiAnalyzer features.	Restricted_User
`adom <adom_name(s)>`	Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiAnalyzer GUI. For more information, see Administrative Domains on page 41.	
`policy-package {<adom name>: <policy package id> <adom policy folder name>/ <package name> | all_policy_ packages}`	Policy package access.	
`restrict-access {enable | disable}`	Enable/disable restricted access to the device VDOM.	disable
`description <string>`	Enter a description for this administrator account. When using spaces, enclose description in quotes.	
`user_type {group | local | pki-auth | radius | ldap | tacacs-plus}`	Enter `local` if the FortiAnalyzer system verifies the administrator's password. Enter `radius` if a RADIUS server verifies the administrator's password.	local
`ldap-server <string>`	Enter the LDAP server name if the user type is set to LDAP.	
`radius_server <string>`	Enter the RADIUS server name if the user type is set t o RADIUS.	

Variable	Description	Default
`tacacs-plus-server <string>`	Enter the TACACS+ server name if the user type is set to TACACS+.	
`group <group_name>`	Enter the administrator group name.	

`ssh-public-key1 <key-type> <key-value>`
`ssh-public-key2 <key-type>, <key-value>`
`ssh-public-key3 <key-type>, <key-value>`
	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application.
	`<key type>`
	The `ssh-dss` for a DSA key, `ssh-rsa` for an RSA key.
	`<key-value>`
	The public key string of the SSH client.	

`wildcard {enable | disable}`	Enable/disable wildcard remote authentication	
`radius-accprofile-override {enable | disable}`	Enable/disable allowing access profile to be overridden from RADIUS.	
`radius-adom-override {enable | disable}`	Enable/disable allowing an ADOM to be overridden from RADIUS.	
`radius-group-match <string>`	Only admin that belong to this group are allowed to login.	
`password-expire <yyyy-mm-dd>`	When enforcing the password policy, enter the date that the current password will expire.	
`force-password-change {enable | disable}`	Enable/disable force password change on next login.	
`subject <string>`	PKI user certificate name constraints. This command is available when a PKI administrator account is configured.	
`ca <string>`	PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured.	
`two-factor-auth {enable | disable}`	Enable/disable two-factor authentication (certificate + password). This command is available when a PKI administrator account is configured.	
`last-name <string>`	Administrator's last name.	

Variable	Description	Default
`first-name <string>`	Administrator's first name.	
`email-address <string>`	Administrator's email address.	
`phone-number <string>`	Administrator's phone number.	
`mobile-number <string>`	Administrator's mobile phone number.	
`pager-number <string>`	Administrator's pager number.	
Variables for `config meta-data` **subcommand**: This subcommand can only change the value of an existing field. To create a new metadata field, use the `config meta-data` command.		
`fieldname`	The label/name of the field. Read-only.	50
`fieldlength`	The maximum number of characters allowed for this field. Read-only.	
`fieldvalue <string>`	Enter a pre-determined value for the field. This is the only value that can be changed with the `config meta-data` subcommand.	
`importance`	Indicates whether the field is compulsory (`required`) or optional (`optional`). Read-only.	optional
`status`	For display only. Value cannot be changed.	enabled
Variables for `config dashboard-tabs` **subcommand**:		
`tabid <integer>`	Tab ID.	
`name <string>`	Tab name.	
Variables for `config dashboard` **subcommand**: You can use this command to create custom dashboards for each administrator.		

Variable	Description	Default
`moduleid`	Widget ID. Enter the module ID of the widget you want to edit. • `1`: System Information • `2`: System Resources • `3`: Device Summary • `4`: Unit Operation • `5`: Alert Message Console • `6`: License Information • `7`: Logs/Data Received • `8`: Log Receive Monitor • `9`: Statistics • `10`: CLI Console • `11`:Insert Rate vs Receive Rate • `12`:Log Insert Lag Time	
`name <string>`	Set the widget name. You can use this command to rename the widgets displayed on the dashboard.	
`column <column_pos>`	Set the widget's column ID.	1 or 2
`refresh-inverval <integer>`	Set the widget's refresh interval.	0
`status {close | open}`	Set the widget's opened/closed status.	open
`tabid <integer>`	Set the ID of the tab where the widget is displayed.	0
`widget-type {alert | devsummary | jsconsole | licinfo | logrecv | raid | rpteng | statisctics | sysinfo | sysop | sysres | top-lograte}`	Set the widget type. Enter one of the following: • `alert`: Alert Message Console • `devsummary`: Device Summary • `jsconsole`: CLI Console • `licinfo`: License Information • `logrecv`: Logs/Data Received • `raid`: Disk Monitor • `rpteng`: Report Engine • `statistics`: Statistics • `sysinfo`: System Information • `sysop`: Unit Operation • `sysres`: System Resources • `top-lograte`: Log Receive Monitor	
`log-rate-type {device | log}`	Log receive monitor widget's statistics breakdown options.	

Variable	Description	Default
`log-rate-topn {1 | 2 | 3 | 4 | 5}`	Log receive monitor widget's number of top items to display.	
`log-rate-period {1hour | 2min | 6hours}`	Log receive monitor widget's data period.	
`res-view-type {history | real-time}`	Widget's data view type.	
`res-period {10min | day | hour}`	Widget's data period. Can be set to 10 minutes, one day, or one hour.	
`num-entries <integer>`	Number of entries.	
`res-cpu-display {average | each}`	Set the widget's CPU display type. Select either: • `average`: Average of all CPUs. • `each`: Display each CPU separately.	
`time-period {1hour | 24hour | 8hour}`	Set the Log Database Monitor widget's data period.	
Variable for `config restrict-dev-vdom` subcommand:		
`dev-vdom <string>`	Enter device or VDOM to edit.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin user
```

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiAnalyzer system does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Example

Use the following commands to add a new administrator account named `admin_2` with the password set to `p8ssw0rd` and the `Super_User` access profile. Administrators that log in to this account will have administrator access to the FortiAnalyzer system from any IP address.

```
config system admin user
```

```
edit admin_2
   set description "Backup administrator"
   set password p8ssw0rd
   set profileid Super_User
end
```

aggregation-client

Use the following commands to configure log aggregation.

Syntax

```
config system aggregation-client
   edit <id>
      set mode {aggregation | both | disable | realtime}
      set agg-password <password>
      set server-ip <ipv4_address>
      set agg-archive-types {Web_Archive | Email_Archive | File_Transfer_Archive | IM_
          Archive | MMS_Archive | AV_Quarantine | IPS_Packets}
      set agg-logtypes {none | app-ctrl | attack | content | dlp | emailfilter |
          event | history | traffic | virus | webfilter | netscan}
      set agg-time <integer>
      set fwd-facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
          kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 |
          local7 | lpr | mail | news | ntp | syslog | user | uucp}
      set fwd-log-source-ip {local_ip | original_ip}
      set fwd-min-level {alert | critical | debug | emergency | error | information |
          notification | warning}
      set fwd-remote-server {cef | fortianalyzer | syslog}
      set fwd-reliable {enable | disable}
      set server-device <string>
      set server-name <string>
      set server-port <integer>
      config device-filter
         edit id
            set action {exclude | include}
            set device <string>
         end
   end
```

Variable	Description
`<id>`	Enter the log aggregation ID that you want to edit. Enter `edit ?` to view available entries.
`mode {aggregation | both | disable | realtime}`	Log aggregation mode: • `aggregation`: Aggregate logs to FortiAnalyzer • `both`: Forward and aggregate logs to the FortiAnalyzer • `disable`: Do not forward or aggregate logs • `realtime`: Real time forward logs to the FortiAnalyzer

Variable	Description
`agg-password <password>`	Log aggregation access password for server. Command only available when the mode is set to `aggregation` or `both`.
`server-ip <ipv4_address>`	Remote server IP address. Command only available when the mode is set to `aggregation`, `both`, or `realtime`.
`agg-archive-types {Web_Archive | Email_Archive | File_Transfer_Archive | IM_Archive | MMS_Archive | AV_Quarantine | IPS_Packets}`	Archive type. Command only available when the mode is set to `aggregation` or `both`.
`agg-logtypes {none | app-ctrl | attack | content | dlp | emailfilter | event | history | traffic | virus | webfilter | netscan}`	Log type. Command only available when the mode is set to `aggregation` or `both`.
`agg-time <integer>`	Daily at the selected time. Command only available when the mode is set to `aggregation` or `both`.

Variable	Description
`fwd-facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}`	Facility for remote syslog. The command is only available when the mode is set to `realtime` or `both`. Select one of the following: • `alert`: Log alert • `audit`: Log audit • `auth`: Security/authorization messages • `authpriv`: Security/authorization messages (private) • `clock`: Clock daemon • `cron`: cron daemon • `daemon`: System daemons • `ftp`: FTP daemon • `kernel`: Kernel messages • `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, `local7`: Reserved for local use • `lpr`: Line printer subsystem • `mail`: Mail system • `news`: Network news subsystem • `ntp`: NTP daemon • `syslog`: Messages generated internally by `syslogd` • `user`: Random user level messages • `uucp`: Network news subsystem
`fwd-log-source-ip {local_ip | original_ip}`	The logs source IP address. Command only available when the mode is set to `realtime` or `both`. Select one of the following: • `local_ip`: Use local IP • `original_ip`: Use original source IP
`fwd-min-level {alert | critical | debug | emergency | error | information | notification | warning}`	Forward logs more sever than this level. This command only available when the mode is set to `realtime` or `both`.
`fwd-remote-server {cef | fortianalyzer | syslog}`	Forwarding all logs to a CEF (Common Event Format) server, syslog server, or the FortiAnalyzer device. This command only available when the mode is set to `realtime` or `both`.
`fwd-reliable {enable | disable}`	Enable/disable reliable logging. set fwd-reliable enable remote server must by syslog server to support reliable forwarding. This command only available when the mode is set to `both` or `real-time`.

Variable	Description
`server-device <string>`	Log aggregation server device ID.
`server-name <string>`	Log aggregation server name.
`server-port <integer>`	Enter the server listen port. This command is available when the mode is set to `both` or `realtime`.
Variables for `config device-filter` subcommand:	
`id`	Enter the device filter ID or enter a number to create a new entry.
`action {exclude | include}`	Select to exclude or include the specified device.
`device <string>`	Select All_FortiGates, All_FortiMail, All_FortiWebs, All_FortiCaches, All_FortiSandboxes, All_Syslogs, or specify specific devices.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system aggregation-client
```

aggregation-service

Use the following commands to configure log aggregation service.

Syntax

```
config system aggregation-service
   set accept-aggregation {enable | disable}
   set accept-realtime-log {enable | disable}
   set aggregation-disk-quota <integer>
   set password <password>
end
```

Variable	Description
`accept-aggregation {enable | disable}`	Enable/disable accept log aggregation option.
`accept-realtime-log {enable | disable}`	Enable to accept real time logs.

Variable	Description
`aggregation-disk-quota <integer>`	Aggregated device disk quota (MB) on server. `accept-aggregation` must be enabled.
`password <password>`	Log aggregation access password for server. `accept-aggregation` must be enabled.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system aggregation-service
```

alert-console

Use this command to configure the alert console options. The alert console appears on the dashboard in the GUI.

Syntax

```
config system alert-console
   set period <integer>
   set severity-level {debug | information | notify | warning | error | critical |
       alert | emergency}
end
```

Variable	Description	Default
`period <integer>`	Enter the number of days to keep the alert console information on the dashboard in days between 1 and 7.	7
`severity-level {debug | information | notify | warning | error | critical | alert | emergency}`	Enter the severity level to display on the alert console on the dashboard.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system alert-console
```

Example

This example sets the alert console message display to warning for a duration of three days.

```
config system alert-console
   set period 3
   set severity-level warning
end
```

alert-event

Use `alert-event` commands to configure the FortiAnalyzer unit to monitor logs for log messages with certain severity levels, or information within the logs. If the message appears in the logs, the FortiAnalyzer unit sends an email or SNMP trap to a predefined recipient(s) of the log message encountered. Alert event messages provide immediate notification of issues occurring on the FortiAnalyzer unit.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server. name

Syntax

```
config system alert-event
   edit <name>
   config alert-destination
      edit destination_id <integer>
         set type {mail | snmp | syslog}
         set from <email_address>
         set to <email_address>
         set smtp-name <server_name>
         set snmp-name <server_name>
         set syslog-name <server_name>
      end
      set enable-generic-text {enable | disable}
      set enable-severity-filter {enable | disable}
      set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
      set generic-text <string>
      set num-events {1 | 5 | 10 | 50 | 100}
      set severity-filter {high | low | medium | medium-high | medium-low}
      set severity-level-comp {>= | = | <=}
      set severity-level-logs {no-check | information | notify | warning | error |
          critical | alert | emergency}
   end
```

Variable	Description	Default
`<name>`	Enter the name of the alert event you want to edit. Enter a new name to create a new entry.	
`destination_id <integer>`	Enter the table sequence number, beginning at 1.	
`type {mail | snmp | syslog}`	Select the alert event message method of delivery.	mail
`from <email_address>`	Enter the email address of the sender of the message. This is available when the `type` is set to `mail`.	
`to <email_address>`	Enter the recipient of the alert message. This is available when the `type` is set to `mail`.	

Variable	Description	Default
`smtp-name <server_name>`	Enter the name of the mail server. This is available when the `type` is set to `mail`.	
`snmp-name <server_name>`	Enter the snmp server name. This is available when the `type` is set to `snmp`.	
`syslog-name <server_name>`	Enter the syslog server name or IP address. This is available when the `type` is set to `syslog`.	
`enable-generic-text {enable | disable}`	Enable/disable the text alert option.	disable
`enable-severity-filter {enable | disable}`	Enable/disable the severity filter option.	disable
`event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}`	The period of time in hours during which if the threshold number is exceeded, the event will be reported. Select one of the following: • `0.5`: 30 minutes • `1`: 1 hour • `3`: 3 hours • `6`: 6 hours • `12`: 12 hours • `24`: 1 day • `72`: 3 days • `168`: 1 week	0.5
`generic-text <string>`	Enter the text the alert looks for in the log messages.	
`num-events {1 | 5 | 10 | 50 | 100}`	Set the number of events that must occur in the given interval before it is reported.	1
`severity-filter {high | low | medium | medium-high | medium-low}`	Set the alert severity indicator for the alert message the FortiAnalyzer unit sends to the recipient. Select one of the following: • `high`: High level alert • `low`: Low level alert • `medium`: Medium level alert • `medium-high`: Medium-high level alert • `medium-low`: Medium-low level alert.	high

Variable	Description	Default
`severity-level-comp {>= | = | <=}`	Set the severity level in relation to the log level. Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than, and equal to (>=) the Warning log level.	=
`severity-level-logs {no-check | information | notify | warning | error | critical | alert | emergency}`	Set the log level the FortiAnalyzer looks for when monitoring for alert messages. Select one of the following: • `no-check`: Do not check the severity level for this log type. • `information` • `notify` • `warning` • `error` • `critical` • `alert` • `emergency`	no-check

Use the show command to display the current configuration if it has been changed from its default value:

```
show system alert-event
```

Example

In the following example, the alert message is set to send an email to the administrator when 5 warning log messages appear over the span of three hours.

```
config system alert-event
   edit warning
      config alert-destination
         edit 1
            set type mail
            set from fmgr@exmample.com
            set to admin@example.com
            set smtp-name mail.example.com
         end
         set enable-severity-filter enable
         set event-time-period 3
         set severity-level-log warning
         set severity-level-comp =
         set severity-filter medium
   end
```

alertemail

Use this command to configure alert email settings for your FortiAnalyzer unit.

All variables are required if `authentication` is enabled.

Syntax

```
config system alertemail
   set authentication {enable | disable}
   set fromaddress <email-address_string>
   set fromname <name_string>
   set smtppassword <password>
   set smtpport <port_int>
   set smtpserver {<ipv4>|<fqdn_string>}
   set smtpuser <username>
end
```

Variable	Description	Default
`authentication {enable | disable}`	Enable/disable alert email authentication.	enable
`fromaddress <email-address_string>`	The email address the alertmessage is from. This is a required variable.	
`fromname <name_string>`	The SMTP name associated with the email address. To enter a name that includes spaces, enclose the whole name in quotes.	
`smtppassword <password>`	Set the SMTP server password.	
`smtpport <port_int>`	The SMTP server port.	25
`smtpserver {<ipv4>|<fqdn_string>}`	The SMTP server address. Enter either a DNS resolvable host name or an IP address.	
`smtpuser <username>`	Set the SMTP server username.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system alertemail
```

Example

Here is an example of configuring alertemail. Enable authentication, the alert is set in Mr. Customer's name and from his email address, the SMTP server port is the default port(25), and the SMTP server is at IP address of 192.168.10.10.

```
config system alertemail
   set authentication enable
   set fromaddress customer@example.com
   set fromname "Mr. Customer"
   set smtpport 25
   set smtpserver 192.168.10.10
end
```

auto-delete

Automatic deletion policy for logs, reports, archived, and quarantined files.

Syntax

```
config system auto-delete
   config dlp-files-auto-deletion
      set status {enable | disable}
      set value <integer>
      set when {days | hours | months | weeks}
   end
   config quarantine-files-auto-deletion
      set status {enable | disable}
      set value <integer>
      set when {days | hours | months | weeks}
   end
   config log-auto-deletion
      set status {enable | disable}
      set value <integer>
      set when {days | hours | months | weeks}
   end
   config report-auto-deletion
      set status {enable | disable}
      set value <integer>
      set when {days | hours | months | weeks}
   end
end
```

Variable	Description
`dlp-files-auto-deletion`	Automatic deletion policy for DLP archives.
`quarantine-files-auto-deletion`	Automatic deletion policy for quarantined files.
`log-auto-deletion`	Automatic deletion policy for device logs.
`report-auto-deletion`	Automatic deletion policy for reports.
`status {enable | disable}`	Enable/disable automatic deletion.
`value <integer>`	Set the age integer.
`when {days | hours | months | weeks}`	Auto-delete data older that <value> days, hours, months, weeks.

backup

backup all-settings

Use this command to set or check the settings for scheduled backups.

Syntax

```
config system backup all-settings
   set status {enable | disable}
   set server {<ipv4>|<fqdn_str>}
   set user <username_string>
   set directory <directory_string>
   set week_days {monday tuesday wednesday thursday friday saturday sunday}
   set time <hh:mm:ss>
   set protocol {ftp | scp | sftp}
   set passwd <password>
   set cert <string>
   set crptpasswd <password>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable/disable scheduled backups.	disable
`server {<ipv4>|<fqdn_str>}`	Enter the IP address or DNS resolvable host name of the backup server.	
`user <username_string>`	Enter the user account name for the backup server.	
`directory <directory_string>`	Enter the name of the directory on the backup server in which to save the backup file.	
`week_days {monday tuesday wednesday thursday friday saturday sunday}`	Enter days of the week on which to perform backups. You may enter multiple days.	
`time <hh:mm:ss>`	Enter time of day to perform the backup. Time is required in the form <hh:mm:ss>.	
`protocol {ftp | scp | sftp}`	Enter the transfer protocol. Select either: FTP, SCP, or SFTP.	sftp
`passwd <password>`	Enter the password for the backup server.	

Variable	Description	Default
cert <string>	SSH certificate for authentication. Only available if the protocol is set to scp.	
crptpasswd <password>	Optional password to protect backup content	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system backup all-settings
```

Example

This example shows a whack where backup server is 172.20.120.11 using the admin account with no password, saving to the /usr/local/backup directory. Backups are done on Mondays at 1:00pm using ftp.

```
config system backup all-settings
   set status enable
   set server 172.20.120.11
   set user admin
   set directory /usr/local/backup
   set week_days monday
   set time 13:00:00
   set protocol ftp
end
```

central-management

Use this command to set or check the settings for central management.

Syntax

```
config system central-management
   set type {fortimanager}
   set allow-monitor {enable | disable}
   set authorized-manager-only {enable | disable}
   set serial-number <serial_number_string>
   set fmg <string>
   set enc-alogorithm {default | high | low}
end
```

Variable	Description
type {fortimanager}	Type of management server.
allow-monitor {enable | disable}	Enable/disable remote monitoring of the device.

Variable	Description
`authorized-manager-only {enable | disable}`	Enable/disable restricted to authorize manager only setting.
`serial-number <serial_number_string>`	Set the device serial number. You can enter up to 5 serial numbers.
`fmg <string>`	Set the IP address or FQDN of the FortiManager.
`enc-alogorithm {default | high | low}`	Set the SSL communication encryption algorithms. Select one of the following: • `default`: SSL communication with high and medium encryption algorithms • `high`: SSL communication with high encryption algorithms • `low`: SSL communication with low encryption algorithms

Use the show command to display the current configuration if it has been changed from its default value:

```
show system central-management
```

certificate

Use the following commands to configure certificate related settings:

certificate ca	certificate oftp
certificate crl	certificate ssh
certificate local	

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), its sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.
   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
   Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ca
   edit <ca_name>
      set ca <cert>
      set comment <string>
   end
```

Variable	Description
`<ca_name>`	Enter the name of the CA certificate you want to edit. Enter a new name to create a new entry.
`ca <cert>`	Enter or retrieve the CA certificate in PEM format.
`comment <string>`	Enter a descriptive comment. (optional)

To view all of the information about the certificate, use the `get` command:

```
get system certificate ca <ca_name>
```

Use the show command to display the current configuration if it has been changed from its default value:

```
show system certificate ca
```

certificate crl

Use this command to install certificate revocation lists.

Syntax

```
config system certificate crl
   edit <crl_name>
      set comment <string>
      set crl <crl>
end
```

Variable	Description
`<crl_name>`	Enter the name of the CRL you want to edit. Enter a new name to create a new entry.
`crl <crl>`	Enter or retrieve the CRL in PEM format.
`comment <string>`	Enter a descriptive comment. (optional)

To view all of the information about the CRL, use the `get` command:

```
get system certificate crl <crl_name>
```

Use the show command to display the current configuration if it has been changed from its default value:

```
show system certificate crl
```

certificate local

Use this command to install local certificates. When a CA processes your CSR, it sends you the CA certificate, the signed local certificate and the CRL.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.
   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
   Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate local
   edit <cert_name>
      set password <cert_password>
      set comment <comment_text>
      set certificate <cert_PEM>
      set private-key <prkey>
      set csr <csr_PEM>
   end
```

Variable	Description
`<cert_name>`	Enter the name of the local certificate you want to edit. Enter a new name to create a new entry.
`password <cert_password>`	Enter the local certificate password.
`comment <comment_text>`	Enter any relevant information about the certificate.
`certificate <cert_PEM>`	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
`private-key <prkey>`	The private key in PEM format.
`csr <csr_PEM>`	The CSR in PEM format.

To view all of the information about the certificate, use the `get` command:

```
get system certificate local [cert_name]
```

Use the show command to display the current configuration if it has been changed from its default value:

```
show system certificate local
```

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
      set certificate <certificate>
      set comment <string>
      set custom {enable | disable}
      set private-key <key>
   end
```

Variable	Description
`certificate <certificate>`	PEM format certificate.
`comment <string>`	OFTP certificate comment.
`custom {enable | disable}`	Enable/disable custom certificates
`private-key <key>`	PEM format private key.

certificate ssh

Use this command to install SSH certificates.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.
   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
5. Use the `system certificate SSH` command to install the SSH certificate.

Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ssh
   edit <name>
      set comment <comment_text>
      set certificate <certificate>
      set private-key <key>
end
```

Variable	Description
`<name>`	Enter the name of the SSH certificate you want to edit. Enter a new name to create a new entry.
`comment <comment_text>`	Enter any relevant information about the certificate.
`certificate <certificate>`	Enter the signed SSH certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
`private-key <key>`	The private key in PEM format.

To view all of the information about the certificate, use the `get` command:

```
get system certificate ssh [cert_name]
```

Use the show command to display the current configuration if it has been changed from its default value:

```
show system certificate ssh
```

dns

Use this command to set the DNS server addresses. Several FortiAnalyzer functions, including sending alert email, use DNS.

Syntax

```
config system dns
   set primary <ipv4_address>
   set secondary <ipv4_address>
end
```

Variable	Description	Default
`primary <ipv4_address>`	Enter the primary DNS server IPv4 address.	208.91.112.53
`secondary <ipv4_address>`	Enter the secondary DNS IPv4 server address.	208.91.112.63

Use the show command to display the current configuration if it has been changed from its default value:

```
show system dns
```

Example

This example shows how to set the primary FortiAnalyzer DNS server IP address to `172.20.120.99` and the secondary FortiAnalyzer DNS server IP address to `192.168.1.199`.

```
config system dns
   set primary 172.20.120.99
```

```
    set secondary 192.168.1.199
end
```

fips

Use this command to set the Federal Information Processing Standards (FIPS) status. FIPS mode is an enhanced security option for some FortiAnalyzer models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.

Syntax

```
config system fips
   set status {enable | disable}
   set fortitrng {enable | disable} | dynamic]
   set re-seed-interval <integer>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable/disable the FIPS-CC mode of operation.	enable
`fortitrng {enable | disable} | dynamic]`	Configure support for the FortiTRNG entropy token: • `enable`: The token must be present during boot up and reseeding. If the token is not present, the boot up or reseeding is interrupted until the token is inserted. • `disable`: The current entropy implementation is used to seed the Random Number Generator (RNG). • `dynamic`: The token is used to seed or reseed the RNG if it is present. If the token is not present, the boot process is not blocked and the old entropy implementation is used.	disable
`re-seed-interval <integer>`	The amount of time, in minutes, between RNG reseeding.	1440

global

Use this command to configure global settings that affect miscellaneous FortiAnalyzer features.

Syntax

```
config system global
   set admin-https-pki-required {enable | disable}
   set admin-lockout-duration <integer>
   set admin-lockout-threshold <integer>
   set admin-maintainer {enable | disable}
   set admintimeout <integer>
   set adom-mode {advanced | normal}
   set adom-status {enable | disable}
```

```
    set auto-register-device {enable | disable}
    set backup-compression {high | low | none | none}
    set backup-to-subfolders {enable | disable}
    set clt-cert-req {enable | disable}
    set console-output {more | standard}
    set daylightsavetime {enable | disable}
    set default-disk-quota <integer>
    set enc-algorithm {high | low | medium}
    set hostname <string>
    set language {english | japanese | simch | trach}
    set ldapconntimeout <integer>
    set log-checksum {md5 | md5-auth | none}
    set log-mode {analyzer | collector}
    set max-concurrent-users <integer>
    set max-running-reports <integer>
    set max-aggregation-taks <integer>
    set pre-login-banner {enable | disable}
    set pre-login-banner-message <string>
    set remoteauthtimeout <integer>
    set search-all-adoms {enable | disable}
    set ssl-low-encryption {enable | disable}
    set ssl-protocol {tlsv1 | sslv3}
    set swapmem {enable | disable}
    set task-list-size <integer>
    set timezone <timezone_int>
    set unregister-pop-up {enable | disable}
    set webservice-proto {tlsv1 | sslv3 | sslv2}
end
```

Variable	Description	Default
`admin-https-pki-required {enable | disable}`	Enable/disable HTTPS login page when PKI is enabled. When enabled, admin users have to provide a valid certificate. When disabled, admin users can login using a valid certificate or password.	disable
`admin-lockout-duration <integer>`	Set the lockout duration (seconds) for FortiAnalyzer administration.	60
`admin-lockout-threshold <integer>`	Set the lockout threshold for FortiAnalyzer administration (1 to 10).	3
`admin-maintainer {enable | disable}`	Enable/disable the special user maintainer. When disabled the maintainer user can not log into the device.	enable
`admintimeout <integer>`	Set the administrator idle timeout (in minutes).	5
`adom-mode {advanced | normal}`	Set the ADOM mode.	normal

Variable	Description	Default
`adom-status {enable | disable}`	Enable/disable ADOMs. ADOMs cannot be disabled until all non-root and non-others ADOMs have been deleted.	disable
`auto-register-device {enable | disable}`	Enable/disable device auto registration by log message.	enable
`backup-compression {high | low | none | none}`	Set the compression level. Select one of: • `high`: Best compression (slowest) • `low`: Low compression (fastest) • `none`: No compression • `normal`: Normal compression	normal
`backup-to-subfolders {enable | disable}`	Enable/disable creation of subfolders on server for backup storage.	disable
`clt-cert-req {enable | disable}`	Enable/disable client certificates for GUI log in.	disable
`console-output {more | standard}`	Select how the output is displayed on the console. Select `more` to pause the output at each full screen until keypress. Select `standard` for continuous output without pauses.	standard
`daylightsavetime {enable | disable}`	Enable/disable daylight saving time. If you enable daylight saving time, the FortiAnalyzer unit automatically adjusts the system time when daylight saving time begins or ends.	enable
`default-disk-quota <integer>`	Default disk quota (MB) for auto-registered device.	1000
`enc-algorithm {high | low | medium}`	Set SSL communication encryption algorithms. Select one of the following: • `high`: SSL communication using high encryption algorithms. • `low`: SSL communication using all available encryption algorithms. • `medium`: SSL communication using high and medium encryption algorithms.	low
`hostname <string>`	Enter the FortiAnalyzer host name.	
`language {english | japanese | simch | trach}`	Web interface language. Select from English, Japanese, Simplified Chinese, or Traditional Chinese.	english

Variable	Description	Default
`ldapconntimeout <integer>`	LDAP connection timeout (in milliseconds).	60000
`log-checksum {md5 | md5-auth | none}`	Record log file hash value, timestamp, and authentication code at transmission or rolling. Select one of the following: • `md5`: Record log file's MD5 hash value only • `md5-auth`: Record log file's MD5 hash value and authentication code • `none`: Do not record the log file checksum	
`log-mode {analyzer | collector}`	Log system operation mode.	
`max-concurrent-users <integer>`	Maximum number of concurrent administrators.	20
`max-running-reports <integer>`	Maximum running reports number (from 1 to 10).	
`max-aggregation-taks <integer>`	Maximum log aggregation task number (from 1 to 10)	
`pre-login-banner {enable | disable}`	Enable/disable the pre-login banner.	
`pre-login-banner-message <string>`	The pre-login banner message.	
`remoteauthtimeout <integer>`	Remote authentication (RADIUS/LDAP) timeout (in seconds).	10
`search-all-adoms {enable | disable}`	Enable/disable search all ADOMS for where-used query.	
`ssl-low-encryption {enable | disable}`	Enable/disable low-grade (40-bit) encryption.	enable
`ssl-protocol {tlsv1 | sslv3}`	Set the SSL protocols. • `tlsv1`: Enable TLSv1 • `sslv3`: Enable SSLv3	
`swapmem {enable | disable}`	Enable/disable virtual memory.	enable
`task-list-size <integer>`	Set the maximum number of completed tasks to keep.	2000

Variable	Description	Default
`timezone <timezone_int>`	The time zone for the FortiAnalyzer unit. See Time zones on page 81.	04 (GMT-8) Pacific Time (US & Canada)
`unregister-pop-up {enable | disable}`	Enable/disable unregistered device popup message in the GUI.	
`webservice-proto {tlsv1 | sslv3 | sslv2}`	Web service connection support SSL protocols. • `tlsv1`: Web Service connection using TLSv1 protocol. • `sslv3`: Web Service connection using SSLv3 protocol. • `sslv2`: Web Service connection using SSLv2 protocol.	`tlsv1`

Use the show command to display the current configuration if it has been changed from its default value:

```
show system global
```

Example

The following command turns on daylight saving time, sets the FortiAnalyzer unit name to FMG3k, sets the LCD password to 123856, and chooses the Eastern time zone for US & Canada.

```
config system global
   set daylightsavetime enable
   set hostname FMG3k
   set lcdpin 123856
   set timezone 12
end
```

Time zones

Integer	Time zone	Integer	Time zone
00	(GMT-12:00) Eniwetak, Kwajalein	41	(GMT+3:30) Tehran
01	(GMT-11:00) Midway Island, Samoa	42	(GMT+4:00) Abu Dhabi, Muscat
02	(GMT-10:00) Hawaii	43	(GMT+4:00) Baku
03	(GMT-9:00) Alaska	44	(GMT+4:30) Kabul
04	**(GMT-8:00) Pacific Time (US & Canada)**	45	(GMT+5:00) Ekaterinburg

Integer	Time zone	Integer	Time zone
05	(GMT-7:00) Arizona	46	(GMT+5:00) Islamabad, Karachi,Tashkent
06	(GMT-7:00) Mountain Time (US & Canada)	47	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
07	(GMT-6:00) Central America	48	(GMT+5:45) Kathmandu
08	(GMT-6:00) Central Time (US & Canada)	49	(GMT+6:00) Almaty, Novosibirsk
09	(GMT-6:00) Mexico City	50	(GMT+6:00) Astana, Dhaka
10	(GMT-6:00) Saskatchewan	51	(GMT+6:00) Sri Jayawardenapura
11	(GMT-5:00) Bogota, Lima, Quito	52	(GMT+6:30) Rangoon
12	(GMT-5:00) Eastern Time (US & Canada)	53	(GMT+7:00) Bangkok, Hanoi, Jakarta
13	(GMT-5:00) Indiana (East)	54	(GMT+7:00) Krasnoyarsk
14	(GMT-4:00) Atlantic Time (Canada)	55	(GMT+8:00) Beijing,ChongQing, HongKong,Urumqi
15	(GMT-4:00) La Paz	56	(GMT+8:00) Irkutsk, Ulaanbaatar
16	(GMT-4:00) Santiago	57	(GMT+8:00) Kuala Lumpur, Singapore
17	(GMT-3:30) Newfoundland	58	(GMT+8:00) Perth
18	(GMT-3:00) Brasilia	59	(GMT+8:00) Taipei
19	(GMT-3:00) Buenos Aires, Georgetown	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
20	(GMT-3:00) Nuuk (Greenland)	61	(GMT+9:00) Yakutsk
21	(GMT-2:00) Mid-Atlantic	62	(GMT+9:30) Adelaide
22	(GMT-1:00) Azores	63	(GMT+9:30) Darwin
23	(GMT-1:00) Cape Verde Is	64	(GMT+10:00) Brisbane
24	(GMT) Casablanca, Monrovia	65	(GMT+10:00) Canberra, Melbourne, Sydney
25	(GMT) Greenwich Mean Time:Dublin, Edinburgh, Lisbon, London	66	(GMT+10:00) Guam, Port Moresby

Integer	Time zone	Integer	Time zone
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	67	(GMT+10:00) Hobart
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	68	(GMT+10:00) Vladivostok
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris	69	(GMT+11:00) Magadan
29	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb	70	(GMT+11:00) Solomon Is., New Caledonia
30	(GMT+1:00) West Central Africa	71	(GMT+12:00) Auckland, Wellington
31	(GMT+2:00) Athens, Istanbul, Minsk	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is
32	(GMT+2:00) Bucharest	73	(GMT+13:00) Nuku'alofa
33	(GMT+2:00) Cairo	74	(GMT-4:30) Caracas
34	(GMT+2:00) Harare, Pretoria	75	(GMT+1:00) Namibia
35	(GMT+2:00) Helsinki, Riga,Tallinn	76	(GMT-5:00) Brazil-Acre)
36	(GMT+2:00) Jerusalem	77	(GMT-4:00) Brazil-West
37	(GMT+3:00) Baghdad	78	(GMT-3:00) Brazil-East
38	(GMT+3:00) Kuwait, Riyadh	79	(GMT-2:00) Brazil-DeNoronha
39	(GMT+3:00) Moscow, St.Petersburg, Volgograd		
40	(GMT+3:00) Nairobi		

interface

Use this command to edit the configuration of a FortiAnalyzer network interface.

Syntax

```
config system interface
   edit <port_string>
      set status {up | down}
      set ip <ipv4address_mask>
      set allowaccess {aggregator http https ping snmp ssh telnet webservice}
      set speed {1000full | 100full | 100half | 10full | 10half | auto}
```

```
    set description <string>
    set alias <string>
    config ipv6
      set ip6-address <IPv6address prefix>
      set ip6-allowaccess {aggregator http https ping6 snmp ssh telnet webservice}
    end
end
```

Variable	Description	Default
`<port_string>`	`<port_string>` can be set to a port number such as port1, port2, port3, or port4. Different FortiAnalyzer models have different numbers of ports. Enter `edit ?` to view available ports, their status, IP address, and duplex setting.	
`status {up | down}`	Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop.	up
`ip <ipv4address_mask>`	Enter the interface IPv4 address and netmask. The IP address cannot be on the same subnet as any other interface.	
`allowaccess {aggregator http https ping snmp ssh telnet webservice}`	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.	
`speed {1000full | 100full | 100half | 10full | 10half | auto}`	Enter the speed and duplexing the network port uses. Enter `auto` to automatically negotiate the fastest common speed. Select from the following: • `1000full`: 1000Mbps full-duplex • `100full`: 100Mbps full-duplex • `100half`: 100Mbps half-duplex • `10full`: 10Mbps full-duplex • `10half`: 10Mbps half-duplex • `auto`: Auto adjust speed	auto
`description <string>`	Enter a description of the interface.	
`alias <string>`	Enter an alias for the interface.	
`ipv6`	Configure the interface IPv6 settings.	
`ip6-address <IPv6address prefix>`	IPv6 address/prefix of interface.	

Variable	Description	Default
`ip6-allowaccess {aggregator http https ping6 snmp ssh telnet webservice}`	Allow management access to the interface.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system interface
```

Example

This example shows how to set the FortiAnalyzer port1 interface IP address and netmask to `192.168.100.159 255.255.255.0`, and the management access to `ping`, `https`, and `ssh`.

```
config system interface
   edit port1
      set allowaccess ping https ssh
      set ip 192.168.110.26 255.255.255.0
      set status up
   end
```

locallog

Use the following commands to configure local log settings:

- locallog disk setting
- locallog filter
- locallog fortianalyzer setting
- locallog memory setting
- locallog syslogd (syslogd2, syslogd3) setting

locallog disk setting

Use this command to configure the FortiAnalyzer disk settings for uploading log files, including configuring the severity of log levels.

`status` must be enabled to view `diskfull`, `max-log-file-size`, and `upload` variables.

`upload` must be enabled to view/set other `upload*` variables.

Syntax

```
config system locallog disk setting
   set diskfull {nolog | overwrite}
   set status {enable | disable}
   set severity {alert | critical | debug | emergency | error | information |
       notification | warning}
   set max-log-file-size <size_integer>
   set roll-schedule {none | daily | weekly}
   set roll-day <string>
   set roll-time <hh:mm>
   set log-disk-full-percentage <integer>
```

```
    set upload {disable | enable}
    set uploadip <ipv4>
    set server-type {faz | ftp | scp | sftp}
    set uploadport <port_integer>
    set uploaduser <user_string>
    set uploadpass <password>
    set uploaddir <directory_string>
    set uploadtype <event>
    set uploadzip {disable | enable}
    set uploadsched {disable | enable}
    set upload-time <hh:mm>
    set upload-delete-files {disable | enable}
end
```

Variable	Description	Default
`diskfull {nolog | overwrite}`	Enter action to take when the disk is full: • `nolog`: Stop logging when disk full • `overwrite`: Overwrites oldest log entries	overwrite
`status {enable | disable}`	Enter `enable` to begin logging.	disable
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the logging severity level. The FortiAnalyzer unit logs all messages at and above the logging severity level you select. For example, if you select `critical`, the unit logs `critical`, `alert`, and `emergency` level messages.	alert
`max-log-file-size <size_integer>`	Enter the size at which the log is rolled. The range is from 1 to 1024 megabytes.	100
`roll-schedule {none | daily | weekly}`	Enter the period for the scheduled rolling of a log file. If `roll-schedule` is `none`, the log rolls when `max-log-file-size` is reached.	none
`roll-day <string>`	Enter the day for the scheduled rolling of a log file.	none
`roll-time <hh:mm>`	Enter the time for the scheduled rolling of a log file.	none
`log-disk-full-percentage <integer>`	Enter the percentage at which the log disk will be considered full.	
`upload {disable | enable}`	Enable to permit uploading of logs.	disable
`uploadip <ipv4>`	Enter IP address of the destination server.	0.0.0.0

Variable	Description	Default
`server-type {faz | ftp | scp | sftp}`	Enter the type the server to use to store the logs. Select one of the following: • `faz`: Log to FortiAnalyzer • `ftp`: Log to an FTP server • `scp`: Log to an SCP server • `sftp`: Log to an SFTP server	
`uploadport <port_integer>`	Enter the port to use when communicating with the destination server.	21
`uploaduser <user_string>`	Enter the user account on the destination server.	
`uploadpass <password>`	Enter the password of the user account on the destination server.	
`uploaddir <directory_string>`	Enter the destination directory on the remote server.	
`uploadtype <event>`	Enter to upload the event log files.	event
`uploadzip {disable | enable}`	Enable to compress uploaded log files.	disable
`uploadsched {disable | enable}`	Enable to schedule log uploads.	
`upload-time <hh:mm>`	Enter to configure when to schedule an upload.	
`upload-delete-files {disable | enable}`	Enable to delete log files after uploading.	enable

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog disk setting
```

Example

In this example, the logs are uploaded to an upload server and are not deleted after they are uploaded.

```
config system locallog disk setting
   set status enable
   set severity information
   set max-log-file-size 1000MB
   set roll-schedule daily
   set upload enable
   set uploadip 10.10.10.1
```

```
    set uploadport port 443
    set uploaduser myname2
    set uploadpass 12345
    set uploadtype event
    set uploadzip enable
    set uploadsched enable
    set upload-time 06:45
    set upload-delete-file disable
end
```

locallog filter

Use this command to configure filters for local logs. All keywords are visible only when `event` is enabled.

Syntax

```
config system locallog [memory | disk | fortianalyzer | syslogd | syslogd2 | syslogd3]
    filter
    set dvm {enable | disable}
    set event {enable | disable}
    set faz {enable | disable}
    set fmgws {enable | disable}
    set fmgws {enable | disable}
    set iolog {enable | disable}
    set system {enable | disable}
    set fgfm {enable | disable}
    set devcfg {enable | disable}
    set glbcfg {enable | disable}
    set scrmgr {enable | disable}
    set webport {enable | disable}
    set scfw {enable | disable}
    set scply {enable | disable}
    set scvpn {enable | disable}
    set epmgr {enable | disable}
    set rev {enable | disable}
    set dm {enable | disable}
    set rtmon {enable | disable}
    set ha {enable | disable}
    set fmwmgr {enable | disable}
    set fgd {enable | disable}
    set fmlmgr {enable | disable}
    set objcfg {enable | disable}
    set logd {enable | disable}
    set fips {enable | disable}
    set devops {enable | disable}
end
```

Variable	Description	Default
`dvm {enable | disable}`	Enable/disable device manager messages.	disable
`event {enable | disable}`	Enable/disable event log messages.	disable

Variable	Description	Default
`faz {enable | disable}`	Enable/disable FortiAnalyzer log messages.	disable
`fmgws {enable | disable}`	Enable/disable web services log messages.	disable
`iolog {enable | disable}`	Enable/disable debug IO log messages.	disable
`system {enable | disable}`	Enable/disable system manager messages.	disable
`fgfm {enable | disable}`	Enable/disable `FGFM` messages.	disable
`devcfg {enable | disable}`	Enable/disable `devcfg` messages.	disable
`glbcfg {enable | disable}`	Enable/disable `glbcfg` messages.	disable
`scrmgr {enable | disable}`	Enable/disable `scrmgr` messages.	disable
`webport {enable | disable}`	Enable/disable `webport` messages.	disable
`scfw {enable | disable}`	Enable/disable `scfw` messages.	disable
`scply {enable | disable}`	Enable/disable policy console messages.	disable
`scvpn {enable | disable}`	Enable/disable `scvpn` messages.	disable
`epmgr {enable | disable}`	Enable/disable `epmgr` messages.	disable
`rev {enable | disable}`	Enable/disable `rev` messages.	disable
`dm {enable | disable}`	Enable/disable `dm` messages.	disable
`rtmon {enable | disable}`	Enable/disable `rtmon` messages.	disable
`ha {enable | disable}`	Enable/disable high availability messages.	disable

Variable	Description	Default
`fmwmgr {enable | disable}`	Enable/disable `fmwmgr` messages.	disable
`fgd {enable | disable}`	Enable/disable `fgd` messages.	disable
`fmlmgr {enable | disable}`	Enable/disable `fmlmgr` messages.	disable
`objcfg {enable | disable}`	Enable/disable `objcfg` messages.	disable
`logd {enable | disable}`	Enable/disable log daemon status messages.	
`fips {enable | disable}`	Enable/disable log of FIPS status messages.	
`devops {enable | disable}`	Enable/disable managed device operations messages.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog disk filter
```

locallog fortianalyzer setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer unit entered in `system log fortianalyzer`.

The severity threshold required to forward a log message to the FortiAnalyzer unit is separate from event, syslog, and local logging severity thresholds.

Syntax

```
config system locallog fortianalyzer setting
   set severity {emergency | alert | critical | error | warning | notification |
       information | debug}
   set status {disable | enable}
end
```

Variable	Description	Default
`severity {emergency | alert | critical | error | warning | notification | information | debug}`	Enter the severity threshold that a log message must meet or exceed to be logged to the FortiAnalyzer unit.	alert
`status {disable | enable}`	Enable/disable remote logging to the FortiAnalyzer unit.	disable

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog fortianalyzer setting
```

Example

You might enable remote logging to the FortiAnalyzer unit configured. Events at the information level and higher, which is everything except debug level events, would be sent to the FortiAnalyzer unit.

```
config system locallog fortianalyzer setting
   set status enable
   set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes.

Syntax

```
config system locallog memory setting
   set severity {emergency | alert | critical | error | warning | notification |
       information | debug}
   set status <disable | enable>
   set diskfull < >
end
```

Variable	Description	Default
`severity {emergency | alert | critical | error | warning | notification | information | debug}`	Enter to configure the severity level to log files.	alert
`status <disable | enable>`	Enable/disable the memory buffer log.	disable
`diskfull < >`	Select the action to take when the disk is full.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog memory setting
```

Example

This example shows how to enable logging to memory for all events at the notification level and above. At this level of logging, only information and debug events will not be logged.

```
config system locallog memory
   set severity notification
   set status enable
end
```

locallog syslogd (syslogd2, syslogd3) setting

Use this command to configure the settings for logging to a syslog server. You can configure up to three syslogd servers, syslogd, syslogd2 and syslogd3.

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
   set csv {disable | enable}
   set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
       kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 |
       lpr | mail | news | ntp | syslog | user | uucp}
   set severity {emergency | alert | critical | error | warning | notification |
       information | debug}
   set status {enable | disable}
   set syslog-name <string>
end
```

Variable	Description	Default
`csv {disable | enable}`	Enable to produce the log in comma separated value (CSV) format. If you do not enable CSV format the FortiAnalyzer unit produces space separated log files.	disable
`facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}`	Enter the facility type. `facility` identifies the source of the log message to syslog. Change `facility` to distinguish log messages from different FortiAnalyzer units so you can determine the source of the log messages. Available facility types are: • `alert`: log alert • `audit`: log audit • `auth`: security/authorization messages • `authpriv`: security/authorization messages (private) • `clock`: clock daemon • `cron`: cron daemon performing scheduled commands • `daemon`: system daemons running background system processes • `ftp`: File Transfer Protocol (FTP) daemon • `kernel`: kernel messages • `local0` – `local7`: reserved for local use • `lpr`: line printer subsystem • `mail`: email system • `news`: network news subsystem • `ntp`: Network Time Protocol (NTP) daemon • `syslog`: messages generated internally by the syslog daemon	`local7`

Variable	Description	Default
`severity {emergency | alert | critical | error | warning | notification | information | debug}`	Select the logging severity level. The FortiAnalyzer unit logs all messages at and above the logging severity level you select. For example, if you select `critical`, the unit logs `critical`, `alert`, and `emergency` level messages.	
`status {enable | disable}`	Enter `enable` to begin logging.	
`syslog-name <string>`	Enter the syslog server name or IP address.	

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog syslogd setting
```

Example

In this example, the logs are uploaded to a syslog server at IP address `10.10.10.8`. The FortiAnalyzer unit is identified as facility `local0`.

```
config system locallog syslogd setting
   set facility local0
   set server 10.10.10.8
   set status enable
   set severity information
end
```

log

Use the following commands to configure log settings:

- log alert
- log fortianalyzer
- log settings

log alert

Use this command to set log based alert settings.

Syntax

```
config system log alert
   set max-alert-count <integer>
end
```

Variable	Description
max-alert-count <integer>	The alert count range between 100 and 1000.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system log alert
```

log fortianalyzer

Use this command to configure a connection with the FortiAnalyzer unit which will be used as the FortiAnalyzer's remote log server. You must configure the FortiAnalyzer unit to accept web service connections.

Syntax

```
config system log fortianalyzer
   set status {disable | enable}
   set ip <ipv4_address>
   set secure_connection {disable | enable}
   set localid <string>
   set psk <password>
   set username <string>
   set passwd <password>
   set auto_install {enable | disable}
end
```

Variable	Description	Default
status {disable | enable}	Enable/disable to configure the connection to the FortiAnalyzer unit.	disable
ip <ipv4_address>	Enter the IP address of the FortiAnalyzer unit.	
secure_connection {disable | enable}	Enable/disable secure connection with the FortiAnalyzer unit.	
localid <string>	Enter the local ID.	
psk <password>	Enter the preshared key with the FortiAnalyzer unit.	
username <string>	Enter the FortiAnalyzer administrator login that the FortiAnalyzer unit will use to administer the FortiAnalyzer unit.	
passwd <password>	Enter the FortiAnalyzer administrator password for the account specified in `username`.	
auto_install {enable | disable}	Enable to automatically update the FortiAnalyzer settings as they are changed on the FortiAnalyzer unit.	disable

Use the show command to display the current configuration if it has been changed from its default value:

```
show system log fortianalyzer
```

Example

You can configure a secure tunnel for logs and other communications with the FortiAnalyzer unit.

```
config system log fortianalyzer
   set status enable
   set ip 192.168.1.100
   set username admin
   set passwd wert5W34bNg
end
```

log settings

Use this command to configure settings for logs. Use the `rolling-regular` subcommand to configure the log rolling of the device logs.

If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Syntax

```
config system log settings
   set log-file-archive-name {basic | extended}
   set FCH-custom-field1 <string>
   set FCT-custom-field1 <string>
   set FGT-custom-field1 <string>
   set FML-custom-field1 <string>
   set FWB-custom-field1 <string>
   set FAZ-custom-field1 <sting>
   set FSA-custom-field1 <sting>
   set sync-search-timeout <integer>
   config rolling-regular
      set days {fri | mon| sat | sun | thu | tue | wed}
      set del-files {enable | disable}
      set directory <dir_string>
      set file-size <size_int>
      set gzip-format {enable | disable}
      set hour <integer>
      set ip <ipv4_address>
      set ip2 <ipv4_address>
      set ip3 <ipv4_address>
      set log-format {csv | native | text}
      set min <integer>
      set server_type {FTP | SCP | SFTP}
      set upload {enable | disable}
      set upload-hour <hour_integer>
      set upload-mode {backup | mirror}
      set upload-trigger {on-roll | on-schedule}
      set username <string>
      set username2 <string>
      set username3 <string>
      set password <password>
      set password2 <password>
```

```
        set password3 <password>
        set when {daily | weekly | none}
    end
end
```

Variable	Description	Default
`log-file-archive-name {basic | extended}`	The log file name format for archiving, such as backup, upload or download. Options include: • `basic` • `extended`: includes the time and date.	
`FCH-custom-field1 <string>`	Name of custom log field to index.	
`FCT-custom-field1 <string>`	Name of custom log field to index.	
`FGT-custom-field1 <string>`	Name of custom log field to index.	
`FML-custom-field1 <string>`	Name of custom log field to index.	
`FWB-custom-field1 <string>`	Name of custom log field to index.	
`FAZ-custom-field1 <sting>`	Name of custom log field to index.	
`FSA-custom-field1 <sting>`	Name of custom log field to index.	
`sync-search-timeout <integer>`	The maximum number of seconds that a log search session can run in synchronous mode.	
Variables for `config rolling-regular` subcommand:		
`days {fri | mon| sat | sun | thu | tue | wed}`	Log files rolling schedule (days of the week). When `when` is set to `weekly`, you can configure `days`, `hour`, and `min` values.	
`del-files {enable | disable}`	Enable to delete the log files from the FortiAnalyzer hard disk one uploading is complete.	

Variable	Description	Default
`directory <dir_string>`	Select a directory on the upload server where the FortiAnalyzer unit stores the uploaded logs. The maximum length is 128 characters.	
`file-size <size_int>`	The maximum size of the current log file that the FortiAnalyzer unit saves to the disk. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file and starts a new active log file. When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name.	100
`gzip-format {enable | disable}`	Enable to compress the log files using the gzip format.	disable
`hour <integer>`	Log files rolling schedule (hour).	
`ip <ipv4_address>`	Enter the IP address for the first server.	0.0.0.0
`ip2 <ipv4_address>`	Enter the IP address for the second server.	0.0.0.0
`ip3 <ipv4_address>`	Enter the IP address for the third server.	0.0.0.0
`log-format {csv | native | text}`	Format of the uploaded log files. Select from the following: • `csv`: CSV (comma-separated value) format • `native`: Native format (text or compact) • `text`: Text format (convert if necessary)	
`min <integer>`	Log files rolling schedule (minutes).	
`server_type {FTP | SCP | SFTP}`	Select the type of upload server.	FTP
`upload {enable | disable}`	Enable the FortiAnalyzer unit to upload the rolled log file to an FTP site. When selecting yes, use `set host_ip` and `set port_int` to define the FTP location.	disable
`upload-hour <hour_integer>`	Enter the hour that you want to upload the log files. The default is zero. Enter the number, without minutes, in the 24-hour format (0-24).	0

Variable	Description	Default
`upload-mode {backup | mirror}`	Configure upload mode with multiple servers. Servers are attempted and used one after the other upon failure to connect. In `backup` mode, servers are attempted and used one after the other upon failure to connect. In `mirror` mode, all configured servers are attempted and uses.	
`upload-trigger {on-roll | on-schedule}`	Enter what type of trigger will upload log files. The trigger `on-roll` will upload log files whenever they roll. The trigger `on-schedule` will upload log files on a scheduled basis.	on-roll
`username <string>`	Enter the user name for the first upload server. The maximum length is 36 characters.	
`username2 <string>`	Enter the user name for the second upload server. The maximum length is 36 characters.	
`username3 <string>`	Enter the user name for the third upload server. The maximum length is 36 characters.	
`password <password>`	Enter the password for the first upload server user name.	
`password2 <password>`	Enter the password for the second upload server user name.	
`password3 <password>`	Enter the password for the third upload server user name.	
`when {daily | weekly | none}`	Set the frequency of when the FortiAnalyzer unit saves the current log file and starts a new active log file. Select this option if you want to start new log files even if the maximum log file size has not been reached. For example, you want to roll a daily log on a FortiAnalyzer unit that does not see a lot of activity.	none

Use the show command to display the current configuration if it has been changed from its default value:

```
show system log settings
```

Example

The following sub-commands enables log rolling when log files are 100 MB.

```
config system log settings
   config rolling-regular
      set file-size 100
   end
end
```

mail

Use this command to configure mail servers on your FortiAnalyzer unit.

Syntax

```
config system mail
   edit <server>
      set auth {enable | disable}
      set passwd <password>
      set port <integer>
      set user <string>
   end
```

Variable	Description
`<server>`	Enter the name of the mail server.
`auth {enable | disable}`	Enable/disable authentication.
`passwd <password>`	Enter the SMTP account password value.
`port <integer>`	Enter the SMTP server port.
`user <string>`	Enter the SMTP account user name.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system mail
```

ntp

Use this command to configure automatic time setting using a Network Time Protocol (NTP) server.

Syntax

```
config system ntp
   set status {enable | disable}
   set sync_interval <min_str>
   config ntpserver
      edit <id>
         set ntpv3 {disable | enable}
         set server {<ipv4> | <fqdn_string>}
         set authentication {disable | enable}
         set key <password>
         set key-id <integer>
   end
end
```

Variable	Description	Default
`status {enable | disable}`	Enable/disable NTP time setting.	disable
`sync_interval <min_str>`	Enter time, in minutes, how often the FortiAnalyzer unit synchronizes its time with the NTP server.	60
Variables for `config ntpserver` **subcommand**:		
`<id>`	NTP server ID	
`ntpv3 {disable | enable}`	Enable/disable NTPV3.	disable
`server {<ipv4> | <fqdn_string>}`	Enter the IP address or fully qualified domain name of the NTP server.	
`authentication {disable | enable}`	Enable/disable MD5 authentication.	disable
`key <password>`	The authentication key.	
`key-id <integer>`	The key ID for authentication.	0

Use the show command to display the current configuration if it has been changed from its default value:

```
show system ntp
```

password-policy

Use this command to configure access password policies.

Syntax

```
config system password-policy
   set status {disable | enable}
   set minimum-length <integer>
   set must-contain {lower-case-letter | non-alphanumeric | number | upper-case-letter}
   set change-4-characters {disable | enable}
   set expire <integer>
end
```

Variable	Description	Default
`status {disable | enable}`	Enable/disable the password policy.	enable
`minimum-length <integer>`	Set the password's minimum length. Must contain between 8 and 256 characters.	8

Variable	Description	Default
`must-contain {lower-case-letter | non-alphanumeric | number | upper-case-letter}`	Characters that a password must contain. • `lower-case-letter`: The password must contain at least one lower case letter • `non-alphanumeric`: The password must contain at least one non-alphanumeric characters • `number`: The password must contain at least one number • `upper-case-letter`: The password must contain at least one upper case letter.	
`change-4-characters {disable | enable}`	Enable/disable changing at least 4 characters for a new password.	disable
`expire <integer>`	Set the number of days after which admin users' password will expire; 0 means never.	0

Use the show command to display the current configuration if it has been changed from its default value:

```
show system password-policy
```

report

Use the following commands to configure report related settings:

- report auto-cache
- report est-browse-time
- report group
- report setting

report auto-cache

Use this command to view or configure report auto-cache settings.

Syntax

```
config system report auto-cache
   set aggressive-drilldown {enable | disable}
   set aggressive-schedule {enable | disable}
   set drilldown-interval <integer>
   set drilldown-status {enable | disable}
   set order {latest-first | oldest-first}
   set status {enable | disable}
end
```

Variable	Description
`aggressive-drilldown {enable | disable}`	Enable/disable the aggressive drill-down auto-cache.
`aggressive-schedule {enable | disable}`	Enable/disable `auto-cache` on schedule reports aggressively.
`drilldown-interval <integer>`	The time interval in hours for drill-down auto-cache.
`drilldown-status {enable | disable}`	Enable/disable drill-down `auto-cache`.
`order {latest-first | oldest-first}`	The order of which SQL log table is processed first. • `latest-first`: The latest SQL log table is processed first. • `oldest-first`: The oldest SQL log table is processed first.
`status {enable | disable}`	Enable/disable the SQL report auto-cache.

Use the `show` command to display the current configuration if it has been changed from its default value:

```
show system report auto-cache
```

report est-browse-time

Use this command to view or configure report estimated browse time settings.

Syntax

```
config system report est-browse-time
   set max-num-user <integer>
   set status {enable | disable}
end
```

Variable	Description
`max-num-user <integer>`	Set the maximum number of users to estimate browse time.
`status {enable | disable}`	Enable/disable estimating browse time.

Use the `show` command to display the current configuration if it has been changed from its default value:

```
show system report est-browse-time
```

report group

Use this command to view or configure report groups.

Syntax

```
config system report group
   edit <group-id>
      set adom <adom-name>
      set case-insensitive {enable | disable}
      set report-like <string>
      config group-by
         edit <var-name>
            set var-expression <string>
      end
      config chart-alternative
         edit <chart-name>
            set chart-replace <string>
      end
end
```

Variable	Description
`<group-id>`	The group ID.
`adom <adom-name>`	Admin domain name.
`case-insensitive {enable | disable}`	Enable or disable case insensitivity.
`report-like <string>`	Enter the rport pattern.
Variables for `config group-by` subcommand:	
`<var-name>`	Variable name.
`var-expression <string>`	Enter the variable expression.
Variables for `config chart-alternative` subcommand:	
`<chart-name>`	Chart name.
`chart-replace <string>`	Enter the chart replacement.

report setting

Use this command to view or configure the day of the week that the week starts on.

Syntax

```
config system report setting
   set hcache-check
   set max-table-rows <integer>
   set report-priority {low | normal}
   set week-start {mon | sun}
end
```

Variable	Description
hcache-check	
max-table-rows <integer>	Set the maximum number of rows that can be generated in a single table.
report-priority {low | normal}	Set the priority of the SQL report.
week-start {mon | sun}	Set the day that the week starts on, either Sunday or Monday.

Use the `show` command to display the current configuration if it has been changed from its default value:

```
show system report settings
```

route

Use this command to view or configure static routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route
   edit <seq_number>
      set device <port_string>
      set dst <ipv4address_mask>
      set gateway <ipv4_address>
   end
```

Variable	Description
<seq_number>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <port_string>	Enter the port used for this route.
dst <ipv4address_mask>	Enter the IPv4 address and mask for the destination network.
gateway <ipv4_address>	Enter the default gateway IPv4 address for this network.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system route
```

route6

Use this command to view or configure static IPv6 routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route6
   edit <seq_int>
      set device <string>
      set dst <ipv6_prefix>
      set gateway <ipv6_address>
   end
```

Variable	Description
`<seq_int>`	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
`device <string>`	Enter the port used for this route.
`dst <ipv6_prefix>`	Enter the IPv6 address and mask for the destination network.
`gateway <ipv6_address>`	Enter the default gateway IPv6 address for this network.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system route6
```

snmp

Use the following commands to configure SNMP related settings:

- snmp community
- snmp sysinfo
- snmp user

snmp community

Use this command to configure SNMP communities on your FortiAnalyzer unit.

You add SNMP communities so that SNMP managers, typically applications running on computers to monitor SNMP status information, can connect to the FortiAnalyzer unit (the SNMP agent) to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when there is a system restart, or when the log disk is almost full.

You can add up to three SNMP communities, and each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiAnalyzer unit for a different set of events.

Hosts are the SNMP managers that make up this SNMP community. Host information includes the IP address and interface that connects it to the FortiAnalyzer unit.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Part of configuring an SNMP manager is to list it as a host in a community on the FortiAnalyzer unit that it will be monitoring. Otherwise that SNMP manager will not receive any traps or events from the FortiAnalyzer unit, and will be unable to query the FortiAnalyzer unit as well.

Syntax

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
      config hosts
         edit <host_number>
            set interface <interface_name>
            set ip <ipv4_address>
         end
   end
```

Variables	Description	Default
`<index_number>`	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	

Variables	Description	Default
events <events_list>	Enable the events for which the FortiAnalyzer unit should send traps to the SNMP managers in this community. To enable multiple traps enter a space and click the Tab button. • cpu-high-exclude-nice: CPU usage exclude nice threshold. • cpu_high: The CPU usage is too high. • disk_low: The log disk is getting close to being full. • intf_ip_chg: An interface IP address has changed. • lic-gbday: High licensed log GB/day detected. • log-alert: Log based alert message. • log-data-rate: High incoming log data rate detected. • log-rate: High incoming log rate detected. • mem_low: The available memory is low. • raid_changed: The RAID status changed. • sys_reboot: The FortiAnalyzer unit has rebooted.	All events enabled
name <community_name>	Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups. For example the Logging and Reporting group would be interested in the disk_low events, but likely not the other events. The name is included in SNMPv2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.	
query-v1-port <port_number>	Enter the SNMP v1 query port number used when SNMP managers query the FortiAnalyzer unit.	161
query-v1-status {enable | disable}	Enable/disable SNMPv1 queries for this SNMP community.	enable
query-v2c-port <port_number>	Enter the SNMPv2c query port number used when SNMP managers query the FortiAnalyzer unit. SNMPv2c queries will include the name of the community.	161
query-v2c-status {enable | disable}	Enable/disable SNMPv2c queries for this SNMP community.	enable
status {enable | disable}	Enable/disable this SNMP community.	enable
trap-v1-rport <port_number>	Enter the SNMPv1 remote port number used for sending traps to the SNMP managers.	162

Variables	Description	Default
`trap-v1-status {enable | disable}`	Enable/disable SNMPv1 traps for this SNMP community.	enable
`trap-v2c-rport <port_number>`	Enter the SNMPv2c remote port number used for sending traps to the SNMP managers.	162
`trap-v2c-status {enable | disable}`	Enable/disable SNMPv2c traps for this SNMP community. SNMPv2c traps sent out to SNMP managers include the community name.	enable
Hosts variables		
`<host_number>`	Enter the index number of the host in the table. Enter an unused index number to create a new host.	
`interface <interface_name>`	Enter the name of the FortiAnalyzer unit that connects to the SNMP manager.	
`ip <ipv4_address>`	Enter the IPv4 address of the SNMP manager.	0.0.0.0

Use the show command to display the current configuration if it has been changed from its default value:

```
show system snmp community
```

Example

This example shows how to add a new SNMP community named SNMP_Com1. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMP v1 compatible, all v2c functionality is disabled. After the community is configured the SNMP manager, or host, is added. The SNMP manager IP address is 192.168.20.34 and it connects to the FortiAnalyzer unit internal interface.

```
config system snmp community
   edit 1
      set name SNMP_Com1
      set query-v2c-status disable
      set trap-v2c-status disable
      config hosts
         edit 1
            set interface internal
            set ip 192.168.10.34
         end
      end
end
```

snmp sysinfo

Use this command to enable the FortiAnalyzer SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiAnalyzer unit to identify it. When your SNMP manager receives traps from the FortiAnalyzer unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Syntax

```
config system snmp sysinfo
   set contact-info <info_string>
   set description <description>
   set engine-id <string>
   set fortianalyzer-legacy-sysoid <string>
   set location <location>
   set status {enable | disable}
   set trap-high-cpu-threshold <percentage>
   set trap-cpu-high-exclude-nice-threshold <string>
   set trap-low-memory-threshold <percentage>
end
```

Variable	Description	Default
`contact-info <info_string>`	Add the contact information for the person responsible for this FortiAnalyzer unit. The contact information can be up to 35 characters long.	
`description <description>`	Add a name or description of the FortiAnalyzer unit. The description can be up to 35 characters long.	
`engine-id <string>`	Local SNMP engine ID string (maximum 24 characters).	
`fortianalyzer-legacy-sysoid <string>`	Enable to switch back to legacy FortiAnalyzer sysObjectOID.	
`location <location>`	Describe the physical location of the FortiAnalyzer unit. The system location description can be up to 35 characters long.	
`status {enable | disable}`	Enable/disable the FortiAnalyzer SNMP agent.	disable
`trap-high-cpu-threshold <percentage>`	CPU usage when trap is set.	80
`trap-cpu-high-exclude-nice-threshold <string>`	CPU high usage exclude nice when trap is sent.	

Variable	Description	Default
`trap-low-memory-threshold <percentage>`	Memory usage when trap is set.	80

Use the show command to display the current configuration if it has been changed from its default value:

```
show system snmp sysinfo
```

Example

This example shows how to enable the FortiAnalyzer SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
   set status enable
   set contact-info 'System Admin ext 245'
   set description 'Internal network unit'
   set location 'Server Room A121'
end
```

snmp user

Use this command to configure SNMPv3 users on your FortiAnalyzer unit. To use SNMPv3, you will first need to enable the FortiAnalyzer SNMP agent. For more information, see snmp sysinfo on page 109. There should be a corresponding configuration on the SNMP server in order to query to or receive traps from FortiAnalyzer.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Syntax

```
config system snmp user
   edit <name>
      set auth-proto {md5 | sha}
      set auth-pwd <password>
      set events <events_list>
      set notify-hosts <ip>
      set priv-proto {aes | des}
      set priv-pwd <password>
      set queries {enable | disable}
      set query-port <port_number>
      set security-level {auth-no-priv | auth-priv | no-auth-no-priv}
   end
end
```

Variable	Description	Default
`<name>`	Enter a SNMPv3 user name to add, edit, or delete.	
`auth-proto {md5 | sha}`	Authentication protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable. Select one of the following: • `md5`: HMAC-MD5-96 authentication protocol • `sha`: HMAC-SHA-96 authentication protocol	sha

Variable	Description	Default
`auth-pwd <password>`	Password for the authentication protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable.	
`events <events_list>`	Enable the events for which the FortiAnalyzer unit should send traps to the SNMPv3 managers in this community. The `raid_changed` event is only available for devices which support RAID. • `cpu-high-exclude-nice`: CPU usage excluding nice threshold. • `cpu_high`: The CPU usage is too high. • `disk_low`: The log disk is getting close to being full. • `intf_ip_chg`: An interface IP address has changed. • `lic-gdbay`: High licensed log GB/day detected. • `log-alert`: Log based alert message. • `log-data-rate`: High incoming log data rate detected. • `log-rate`: High incoming log rate detected. • `mem_low`: The available memory is low. • `raid_changed`: RAID status changed. • `sys_reboot`: The FortiAnalyzer unit has rebooted.	All events enabled
`notify-hosts <ip>`	Hosts to send notifications (traps) to.	
`priv-proto {aes | des}`	Privacy (encryption) protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable. Select one of the following: • `aes`: CFB128-AES-128 symmetric encryption protocol • `des`: CBC-DES symmetric encryption protocol	aes
`priv-pwd <password>`	Password for the privacy (encryption) protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable.	
`queries {enable | disable}`	Enable/disable queries for this user.	enable
`query-port <port_number>`	SNMPv3 query port.	161

Variable	Description	Default
security-level {auth-no-priv | auth-priv | no-auth-no-priv}	Security level for message authentication and encryption. Select one of the following: • auth-no-priv: Message with authentication but no privacy (encryption) • auth-priv: Message with authentication and privacy (encryption) • no-auth-no-priv: Message with no authentication and no privacy (encryption).	no-auth-no-priv

Use the show command to display the current configuration if it has been changed from its default value:

```
show system snmp user
```

sql

Configure SQL settings.

Syntax

```
config system sql
   set database-name <string>
   set database-type <postres>
   set device-count-high {enable | disable}
   set event-table-partition-time <integer>
   set fct-table-partition-time <integer>
   set logtype {none | app-ctrl | attack | content | dlp | emailfilter | event |
       generic | history | traffic | virus | voip | webfilter | netscan}
   set password <password>
   set prompt-sql-upgrade {enable | disable}
   set rebuild-event {enable | disable}
   set rebuild-event-start-time <hh:mm> <yyyy/mm/dd>
   set resend-device < >
   set reset {enable | disable}
   set server <string>
   set start-time <hh>:<mm> <yyyy>/<mm>/<dd>
   set status {disable | local | remote}
   set text-search-index {enable | disable}
   set traffic-table-partition-time <integer>
   set username <string>
   set utm-table-partition-time <integer>
config custom-index
   edit <id>
      set device-type {FortiCache | FortiGate | FortiMail | FortiSandbox | FortiWeb}
      set index-field <Field-Name>
      set log-type <Log-Type>
   end
config ts-index-field
   edit <category>
      set <value> <string>
   end
end
```

Variable	Description
`database-name <string>`	Remote SQL database name. The maximum length is 64 characters. Command only available when `status` is set to `remote`.
`database-type <postres>`	Database type. Command only available when `status` is set to `local` or `remote`.
`device-count-high {enable | disable}`	Must be set to `enable` if the count of registered devices is greater than 8000.
`event-table-partition-time <integer>`	Maximum SQL database table partitioning time range in minutes (0 for unlimited) for event logs.
`fct-table-partition-time <integer>`	Maximum SQL database table partitioning time range in minutes (0 for unlimited) for FortiClient logs.
`logtype {none | app-ctrl | attack | content | dlp | emailfilter | event | generic | history | traffic | virus | voip | webfilter | netscan}`	Log type. Command only available when `status` is set to `local` or `remote`.
`password <password>`	The password that the Fortinet unit will use to authenticate with the remote database. Command only available when `status` is set to `remote`.
`prompt-sql-upgrade {enable | disable}`	Prompt to convert log database into SQL database at start time on GUI.
`rebuild-event {enable | disable}`	Enable/disable a rebuild event during SQL database rebuilding.
`rebuild-event-start-time <hh:mm> <yyyy/mm/dd>`	The rebuild event starting date and time.
`resend-device {enable | disable}`	Enable to resend logs to the database.
`reset {enable | disable}`	This command is hidden.

Variable	Description
`server <string>`	The IP address or host name of the remote database server. The maximum length is 64 characters. Command only available when `status` is set to `remote`.
`start-time <hh>:<mm> <yyyy>/<mm>/<dd>`	Start date and time <hh:mm yyyy/mm/dd>. Command only available when `status` is set to `local` or `remote`.
`status {disable | local | remote}`	SQL database status.
`text-search-index {enable | disable}`	Enable or diable the text search index.
`traffic-table-partition-time <integer>`	Maximum SQL database table partitioning time range in minutes (0 for unlimited) for traffic logs.
`username <string>`	The user name that the Fortinet unit will use to authenticate with the remote database. The maximum length is 64 characters. Command only available when `status` is set to `remote`.
`utm-table-partition-time`	Maximum SQL database table partitioning time range in minutes (0 for unlimited) for UTM logs.
Variables for `config custom-index` subcommand:	
`device-type {FortiCache | FortiGate | FortiMail | FortiSandbox | FortiWeb}`	Set the device type. Select one of the following: • FortiCache • FortiGate • FortiMail • FortiSandbox • FortiWeb
`index-field <Field-Name>`	Type a valid field name. Select one of the available field names. The available options for `index-field` is dependent on the `device-type` entry.
`log-type <Log-Type>`	Type the log type. The available options for `log-type` is dependent on the `device-type` entry. Select one of the available log types. • FortiCache: N/A • FortiGate: `app-ctrl`, `content`, `dlp`, `emailfilter`, `event`, `netscan`, `traffic`, `virus`, `voip`, `webfilter` • FortiMail: `emailfilter`, `event`, `history`, `virus` • FortiSandbox: N/A • FortiWeb: attack, event, traffic

Variable	Description
Variables for `config ts-index-field` **subcommand**:	
`<category>`	Category of the text search index fields. The following is the list of categories and their default fields. Select one of the following: • `FGT-app-ctrl`: `user`, `group`, `srcip`, `dstip`, `dstport`, `service`, `app`, `action`, `status`, `hostname` • `FGT-attack`: `severity`, `srcip`, `proto`, `user`, `attackname` • `FGT-content`: `from`, `to`, `subject`, `action`, `srcip`, `dstip`, `hostname`, `status` • `FGT-dlp`: `user`, `srcip`, `service`, `action`, `file` • `FGT-emailfilter`: `user`, `srcip`, `from`, `to`, `subject` • `FGT-event`: `subtype`, `ui`, `action`, `msg` • `FGT-traffic`: `user`, `srcip`, `dstip`, `service`, `app`, `utmaction`, `utmevent` • `FGT-virus`: `service`, `srcip`, `file`, `virus`, `user` • `FGT-voip`: `action`, `user`, `src`, `dst`, `from`, `to` • `FGT-webfilter`: `user`, `srcip`, `status`, `catdesc` • `FGT-netscan`: `user`, `dstip`, `vuln`, `severity`, `os` • `FML-emailfilter`: `client_name`, `dst_ip`, `from`, `to`, `subject` • `FML-event`: `subtype`, `msg` • `FML-history`: `classifier`, `disposition`, `from`, `to`, `client_name`, `direction`, `domain`, `virus` • `FML-virus`: `src`, `msg`, `from`, `to` • `FWB-attack`: `http_host`, `http_url`, `src`, `dst`, `msg`, `action` • `FWB-event`: `ui`, `action`, `msg` • `FWB-traffic`: `src`, `dst`, `service`, `http_method`, `msg`
`<value>`	Fields of the text search filter.
`<string>`	Select one or more field names separated with a comma. The available field names is dependent on the category selected.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system sql
```

syslog

Use this command to configure Syslog servers.

Syntax

```
config system syslog
   edit <name>
      set ip <string>
      set port <integer>
   end
end
```

Variable	Description
`<name>`	Syslog server name.
`ip <string>`	Syslog server IP address or hostname.
`port <integer>`	Syslog server port.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system syslog
```

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer unit's built-in FortiGuard Distribution Server (FDS).

This chapter contains following sections:

analyzer	fct-services	server-override-status
av-ips	multilayer	service
device-version	publicnetwork	support-pre-fgt43
disk-quota	server-access-priorities	

analyzer

analyzer virus report

Use this command to enable or disable notification of virus detection to Fortinet.

Syntax

```
config fmupdate analyzer virusreport
   set status {enable | disable}
end
```

Variables	Description	Default
`status {enable | disable}`	Enable/disable sending virus detection notification to Fortinet.	enable

Example

This example enables virus detection notifications to Fortinet.

```
config fmupdate analyzer virusreport
   set status enable
end
```

av-ips

Use the following commands to configure antivirus settings:

av-ips advanced-log
av-ips fct server-override
av-ips fgt server-override
av-ips push-override
av-ips push-override-to-client
av-ips update-schedule
av-ips web-proxy

av-ips advanced-log

Use this command to enable logging of FortiGuard Antivirus and IPS update packages received by the FortiAnalyzer unit's built-in FDS from the FortiGuard Distribution Network (FDN).

Syntax

```
config fmupdate av-ips advanced-log
   set log-fortigate {enable | disable}
   set log-server {enable | disable}
end
```

Variables	Description	Default
`log-fortigate {enable | disable}`	Enable/disable logging of FortiGuard Antivirus and IPS service updates of FortiGate devices.	disable
`log-server {enable | disable}`	Enable/disable logging of update packages received by the built-in FDS server.	disable

Example

Enable logging of FortiGuard Antivirus updates to FortiClient installations and update packages downloaded by the built-in FDS from the FDN.

```
config fmupdate av-ips advanced-log
   set log-forticlient enable
   set log-server enable
end
```

av-ips fct server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard Antivirus updates for FortiClient from the FDN.

Syntax

```
config fmupdate av-ips fct server-override
   set status {enable | disable}
   config servlist
      edit <id>
         set ip <ipv4_address>
         set port <integer>
      end
   end
```

Variables	Description	Default
`status {enable | disable}`	Enable/disable the override.	disable
Keywords and variables for `config servlist` **subcommand**:		
`<id>`	Override server ID (1-10).	
`ip <ipv4_address>`	Enter the IP address of the override server address.	0.0.0.0
`port <integer>`	Enter the port number to use when contacting the FDN.	443

Example

Configure the FortiAnalyzer unit's built-in FDS to use a specific FDN server and a different port when retrieving FortiGuard Antivirus updates for FortiClient from the FDN.

```
config fmupdate av-ips fct server-override
   set status enable
   config servlist
      edit 1
         set ip 192.168.25.152
         set port 80
      end
   end
```

av-ips fgt server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard Antivirus and IPS updates for FortiGate units from the FDN.

Syntax

```
config fmupdate av-ips fgt server-override
   set status {enable | disable}
   config servlist
   edit <id>
      set ip <ipv4_address>
      set port <integer>
   end
end
```

Variables	Description	Default
`status {enable | disable}`	Enable/disable the override.	disable
Keywords and variables for `config servlist` **subcommand**:		
`<id>`	Override server ID (1-10)	

Variables	Description	Default
ip <ipv4_address>	Enter the IP address of the override server address.	0.0.0.0
port <integer>	Enter the port number to use when contacting the FDN.	443

Example

You could configure the FortiAnalyzer unit's built-in FDS to use a specific FDN server and a different port when retrieving FortiGuard Antivirus and IPS updates for FortiGate units from the FDN.

```
config fmupdate av-ips fgt server-override
   set status enable
   config servlist
      edit 1
         set ip 172.27.152.144
         set port 8890
      end
   end
```

av-ips push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDN sends FortiGuard Antivirus and IPS push messages.

This is useful if push notifications must be sent to an IP address and/or port other than the FortiAnalyzer unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiAnalyzer unit.

Syntax

```
config fmupdate av-ips push-override
   set ip <ipv4_address>
   set port <integer>
   set status {enable | disable}
end
```

Variables	Description	Default
ip <ipv4_address>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiAnalyzer unit.	0.0.0.0
port <integer>	Enter the receiving port number on the NAT device.	9443
status {enable | disable}	Enable/disable the push updates.	disable

Example

You could enable the FortiAnalyzer unit's built-in FDS to receive push messages.

If there is a NAT device or firewall between the FortiAnalyzer unit and the FDN, you could also notify the FDN to send push messages to the external IP address of the NAT device, instead of the FortiAnalyzer unit's private network IP address.

```
config fmupdate av-ips push-override
```

```
      set status enable
      set ip 172.16.124.135
      set port 9000
   end
```

You would then configure port forwarding on the NAT device, forwarding push messages received on UDP port 9000 to the FortiAnalyzer unit on UDP port 9443.

av-ips push-override-to-client

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDN sends FortiGuard Antivirus and IPS push messages.

This command is useful if push notifications must be sent to an IP address and/or port other than the FortiAnalyzer unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiAnalyzer unit.

Syntax

```
   config fmupdate av-ips push-override-to-client
      set status {enable | disable}
      config <announce-ip>
         edit <id>
            set ip <ipv4_address>
            set port <integer>
         end
      end
```

Variables	Description	Default
status {enable | disable}	Enable/disable the push updates.	disable
<announce-ip>	Configure the IP information of the device.	
<id>	Edit the announce IP ID.	
ip <ipv4_address>	Enter the announce IP address.	0.0.0.0
port <integer>	Enter the announce IP port.	9443

av-ips update-schedule

Use this command to configure the built-in FDS to retrieve FortiGuard Antivirus and IPS updates at a specified day and time.

Syntax

```
   config fmupdate av-ips update-schedule
      set frequency {every | daily | weekly}
      set status {enable | disable}
      set time <hh:mm>
   end
```

Variables	Description	Default
`frequency {every | daily | weekly}`	Enter to configure the frequency of the updates.	every
`status {enable | disable}`	Enable/disable regularly scheduled updates.	enable
`time <hh:mm>`	Enter the time or interval when the update will begin. For example, if you want to schedule an update every day at 6:00 PM, enter `18:00`. The time period format is the 24-hour clock: hh=0-23, mm=0-59. If the minute is `60`, the updates will begin at a random minute within the hour. If the `frequency` is `every`, the time is interpreted as an hour and minute interval, rather than a time of day.	01:60

Example

You could schedule the built-in FDS to request the latest FortiGuard Antivirus and IPS updates every five hours, at a random minute within the hour.

```
config fmupdate av-ips udpate-schedule
   set status enable
   set frequency every
   set time 05:60
end
```

av-ips web-proxy

Use this command to configure a web proxy if FortiGuard Antivirus and IPS updates must be retrieved through a web proxy.

Syntax

```
config fmupdate av-ips web-proxy
   set ip <ipv4_address>
   set mode {proxy | tunnel}
   set password <password>
   set port <integer>
   set status {enable | disable}
   set username <string>
end
```

Variables	Description	Default
`ip <ipv4_address>`	Enter the IP address of the web proxy.	0.0.0.0
`mode {proxy | tunnel}`	Enter the web proxy mode.	

Variables	Description	Default
`password <password>`	If the web proxy requires authentication, enter the password for the user name.	No default.
`port <integer>`	Enter the port number of the web proxy.	80
`status {enable | disable}`	Enable/disable connections through the web proxy.	disable
`username <string>`	If the web proxy requires authentication, enter the user name.	No default.

Example

You could enable a connection through a non-transparent web proxy on an alternate port.

```
config fmupdate av-ips web-proxy
   set status enable
   set mode proxy
   set ip 10.10.30.1
   set port 8890
   set username avipsupdater
   set password cvhk3rf3u9jvsYU
end
```

device-version

Use this command to configure the correct firmware version of the device or devices connected or that will be connecting to the FortiAnalyzer unit. You should verify what firmware version is currently running on the device before using this command.

Syntax

```
config fmupdate device-version
   set faz <firmware_version>
   set fct <firmware_version>
   set fgt <firmware_version>
   set fml <firmware_version>
   set fsa <firmware_version>
   set fsw <firmware_version>
end
```

Variables	Description
`faz <firmware_version>`	Enter the FortiAnalyzer firmware version. • `3.0`: Support version 3.0 • `4.0`: Support version 4.0 • `5.0`: Support version 5.0 • `6.0`: Support versions greater than 5.0

Variables	Description
`fct <firmware_version>`	Enter the FortiClient firmware version. • `3.0`: Support version 3.0 • `4.0`: Support version 4.0 • `5.0`: Support version 5.0 • `6.0`: Support versions greater than 5.0
`fgt <firmware_version>`	Enter the correct firmware version that is currently running for FortiGate units. • `3.0`: Support version 3.0 • `4.0`: Support version 4.0 • `5.0`: Support version 5.0 • `6.0`: Support versions greater than 5.0
`fml <firmware_version>`	Enter the correct firmware version that is currently running for the FortiMail units. • `3.0`: Support version 3.0 • `4.0`: Support version 4.0 • `5.0`: Support version 5.0 • `6.0`: Support versions greater than 5.0
`fsa <firmware_version>`	Enter the correct firmware version that is currently running for the FortiSandbox units. • `1.0`: Support version 1.0 • `2.0`: Support versions greater than 2.0
`fsw <firmware_version>`	Enter the correct firmware version that is currently running for the FortiSwitch units. • `3.0`: Support version 3.0 • `4.0`: Support version 4.0 • `5.0`: Support version 5.0 • `6.0`: Support versions greater than 5.0

Example

In the following example, the FortiGate units, including FortiClient agents, are configured with the new firmware version 4.0.

```
config fmupdate device-version
   set fct 4.0
   set fgt 4.0
end
```

disk-quota

Use this command to configure the disk space available for use by the Upgrade Manager.

If the Upgrade Manager disk space is full or if there is insufficient space to save an update package to disk, the package will not download and an alert will be sent to notify you.

Syntax

```
config fmupdate disk-quota
   set value <size_int>
end
```

Use `value` to set the size of the Upgrade Manager disk quota in MBytes. The default size is 10 MBytes. If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

Use this command to configure the built-in FDS to provide FortiGuard services to FortiClient installations.

Syntax

```
config fmupdate fct-services
   set status {enable | disable}
   set port <integer>
end
```

Variables	Description	Default
`status {enable | disable}`	Enable/disable built-in FDS service to FortiClient installations.	enable
`port <integer>`	Enter the port number on which the built-in FDS should provide updates to FortiClient installations.	80

Example

You could configure the built-in FDS to accommodate older versions of FortiClient installations by providing service on their required port.

```
config fmupdate fct-services
   set status enable
   set port 80
end
```

multilayer

Use this command for multilayer mode configuration.

Syntax

```
config fmupdate multilayer
   set webspam-rating {disable | enable}
end
```

Variables	Description	Default
`webspam-rating {disable | enable}`	Enable/disable URL/antispam rating service.	enable

publicnetwork

Use this command to enable access to the public FDS. If this function is disabled, the service packages, updates, and license upgrades must be imported manually.

Syntax

```
config fmupdate publicnetwork
   set status {enable | disable}
end
```

Variables	Description	Default
`status {disable | enable}`	Enable/disable the publicnetwork.	enable

server-access-priorities

Use this command to configure how a FortiGate unit may download antivirus updates and request web filtering services from multiple FortiAnalyzer units and private FDS servers.

By default, the FortiGate unit receives updates from the FortiAnalyzer unit if the FortiGate unit is managed by the FortiAnalyzer unit and the FortiGate unit was configured to receive updates from the FortiAnalyzer unit.

Syntax

```
config fmupdate server-access-priorities
   set access-public {disable | enable}
   set av-ips {disable | enable}
end
```

Variables	Description	Default
`access-public {disable | enable}`	Disable to prevent FortiAnalyzer default connectivity to public FDS and FortiGuard servers.	enable
`av-ips {disable | enable}`	Enable to allow the FortiGate unit to get antivirus updates from other FortiAnalyzer units or private FDS servers.	disable

config private-server

Use this command to configure multiple FortiAnalyzer units and private servers.

Syntax

```
config fmupdate server-access-priorities
   config private-server
      edit <id>
         set ip <ipv4_address>
         set time_zone <integer>
      end
   end
```

Variables	Description
<id>	Enter a number to identify the FortiAnalyzer unit or private server.
ip <ipv4_address>	Enter the IP address of the FortiAnalyzer unit or private server.
time_zone <integer>	Enter the correct time zone of the private server. Using -24 indicates that the server is using the local time zone.

Example

The following example configures access to public FDS servers and allows FortiGate units to receive antivirus updates from other FortiAnalyzer units and private FDS servers. This example also configures two private servers.

```
config fmupdate server-access-priorities
   set access-public enable
   set av-ips enable
      config private-server
         edit 1
            set ip 172.16.130.252
         next
         edit 2
            set ip 172.31.145.201
         end
      end
```

server-override-status

Syntax

```
config fmupdate server-override-status
   set mode {loose | strict}
end
```

Variables	Description	Default
`mode {loose | strict}`	Set the server override mode. • `loose`: allow access other servers • `strict`: access override server only).	loose

service

Use this command to enable or disable the services provided by the built-in FDS.

Syntax

```
config fmupdate service
   set avips {enable | disable}
   set use-cert {BIOS | FortiGuard}
end
```

Variables	Description	Default
`avips {enable | disable}`	Enable the built-in FDS to provide FortiGuard Antivirus and IPS updates.	disable
`use-cert {BIOS | FortiGuard}`	Choose local certificate. • `BIOS`: Use default certificate in BIOS. • `FortiGuard`: Use default certificate as FortiGuard.	BIOS

Example

```
config fmupdate service
   set avips enable
end
```

support-pre-fgt43

Use this command to allow support for FortiOS v4.2 and older.

Syntax

```
config fmupdate support-pre-fgt43
   set status {enable | disable}
end
```

Variables	Description	Default
`status {enable | disable}`	Enable/disable support for FortiOS v4.2 and older.	disable

execute

The execute commands perform immediate operations on the FortiAnalyzer unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiAnalyzer unit.
- Start and stop the FortiAnalyzer unit.
- Reset or shut down the FortiAnalyzer unit.

FortiAnalyzer commands and variables are case sensitive.

This chapter contains following sections:

add-vm-license	log-aggregation	sql-local
backup	log-integrity	sql-query-dataset
bootimage	lvm	sql-query-generic
certificate	ping	sql-report
console	ping6	ssh
date	raid	ssh-known-hosts
device	reboot	time
factory-license	remove	top
fgfm	reset	traceroute
fmupdate	reset-sqllog-transfer	traceroute6
format	restore	
log	shutdown	

add-vm-license

Use this command to add a license to your FortiAnalyzer VM.

This command is only available on FortiAnalyzer VM models.

Syntax

```
execute add-vm-license <vmware license>
```

Variable	Description
<vmware license>	Enter the FortiAnalyzer VMware license string.

backup

Use the following commands to backup all settings or logs on your FortiAnalyzer:

backup all-settings	backup logs-rescue
backup logs	backup reports
backup logs-only	backup reports-config

backup all-settings

Backup the FortiAnalyzer unit settings to an FTP, SFTP, or SCP server.

When you back up the unit settings from the vdom_admin account, the backup file contains global settings and the settings for each VDOM. When you back up the unit settings from a regular administrator account, the backup file contains the global settings and only the settings for the VDOM to which the administrator belongs.

Syntax

```
execute backup all-settings {ftp | sftp} <ip> <string> <username> <password> <crpt_
    password_string>
execute backup all-settings <scp> <ip> <string> <username> <ssh-cert> <crpt_password_
    string>
```

Variable	Description
<ip>	Enter the FTP/SFTP/SCP server IP address.
<string>	Enter the file name for the backup and if required, enter the path to where the file will be backed up to on the backup server.
<username>	Enter username to use to log on the backup server.
<password>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certificate used for user authentication. This options is only available when selecting to backup to an SCP server.
<crpt_password_ string>	Enter an encryption key (password) to encrypt data. (optional)

backup logs

Backup device logs to a FTP, SFTP, or SCP server.

Syntax

```
execute backup logs <device name(s)| all> <service> <ip> <user name> <password>
    <directory>
```

Variable	Description
`<device name(s)| all>`	Enter the device name(s) separated by commas, or `all` for all devices. Example: FWF40C3911000061
`<service>`	Select the transfer protocol. Select one of FTP, SFTP, or SCP.
`<ip>`	Enter the server IP address
`<user name>`	Enter the username on the server
`<password>`	Enter the password, or '-' for none.
`<directory>`	Enter the directory on the server, or press `<Enter>` for none.

backup logs-only

Backup device logs only to an FTP, SFTP, or SCP server.

Syntax

```
execute backup logs-only <device name(s)> <service> <ip> <user name> <password>
    <directory>
```

Variable	Description
`<device name(s)>`	Enter the device name(s) separated by commas, or `all` for all devices.
`<service>`	Select the transfer protocol. Select one of FTP, SFTP, or SCP.
`<ip>`	Enter the server IP address
`<user name>`	Enter the username on the server
`<password>`	Enter the password, or '-' for none.
`<directory>`	Enter the directory on the server, or press `<Enter>` for none.

backup logs-rescue

Use this hidden command to backup logs regardless of the DVM database for emergency reasons. This command will scan folders under `/Storage/Logs/` for possible device logs to backup.

Syntax

```
execute backup logs-rescue <device serial number(s)> <service> <ip> <user name>
    <password> <directory>
```

Variable	Description
`<device serial number(s)>`	Enter the device serial number(s) separated by commas, or `all` for all devices. Example: FWF40C3911000061
`<service>`	Select the transfer protocol. Select one of FTP, SFTP, or SCP.
`<ip>`	Enter the server IP address
`<user name>`	Enter the username on the server
`<password>`	Enter the password, or '-' for none.
`<directory>`	Enter the directory on the server, or press `<Enter>` for none.

backup reports

Backup reports to an FTP, SFTP, or SCP server.

Syntax

```
execute backup reports <report schedule name(s)> <report name pattern> <service> <ip>
    <user name> <password> <directory>
```

Variable	Description
`<report schedule name(s)>`	Enter the report name(s) separated by commas, or `all` for all reports.

`<report name pattern>`	Backup reports with names containing given pattern.
	• A '?' matches any single character.
	• A '*' matches any string, including the empty string, e.g.:
	  • foo: for exact match
	  • *foo: for report names ending with foo
	  • foo*: for report names starting with foo
	  • *foo*: for report names containing foo substring

`<service>`	Select the transfer protocol. Select one of: `ftp`,`sftp`, or `scp`.
`<ip>`	Enter the server IP address
`<user name>`	Enter the username on the server
`<password>`	Enter the password, or '-' for none.
`<directory>`	Enter the directory on the server, or press `<Enter>` for none.

backup reports-config

Backup the report configuration to a specified server.

Syntax

```
execute backup <reports-config> {<adom_name> | all]} <service> <ip> <user name>
    <password> <directory>
```

Variable	Description
`{<adom_name> | all]}`	Select to backup a specific ADOM or all ADOMs.
`<service>`	Select the transfer protocol. Select one of: `ftp`,`sftp`, or `scp`.
`<ip>`	Enter the server IP address
`<user name>`	Enter the username on the server
`<password>`	Enter the password, or '-' for none.
`<directory>`	Enter the directory on the server, or press `<Enter>` for none.

bootimage

Set the image from which the FortiAnalyzer unit will boot the next time it is restarted.

Syntax

```
execute bootimage {primary | secondary}
```

Variable	Description
`{primary | secondary}`	Select to boot from either the primary or secondary partition.

If you do not specify primary or secondary, the command will report whether it last booted from the primary or secondary boot image.

If your FortiAnalyzer unit does not have a secondary image, the bootimage command will inform you that option is not available.

To reboot your FortiAnalyzer unit, use:

```
execute reboot
```

This command is only available on hardware-based FortiAnalyzer models.

certificate

Use these commands to manage certificates:

- certificate ca
- certificate local

certificate ca

Use these commands to list CA certificates, and to import or export CA certificates.

Syntax

To list the CA certificates installed on the FortiAnalyzer unit:

```
execute certificate ca list
```

To export or import CA certificates:

```
execute certificate ca {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
list	Generate a list of CA certificates on the FortiAnalyzer system.
<cert_name>	Enter the name of the certificate.
<tftp_ip>	Enter the IP address of the TFTP server.

certificate local

Use these commands to list, import, export, and generate local certificates.

Syntax

To list the local certificates installed on the FortiAnalyzer unit:

```
execute certificate local list
```

To export or import local certificates:

```
execute certificate local {<export>|<import>} <cert_name> <tftp_ip>
```

To generate local certificates:

```
execute certificate local generate <certificate-name_str> <key_size> <subject>
    <country> <state> <city> <org> <unit> <email>
```

Variable	Description
<export>	Export CA certificate to TFTP server.

Variable	Description
<import>	Import CA certificate from a TFTP server.
list	Generate a list of CA certificates on the FortiAnalyzer system.
generate	Generate a certificate request (X.509 certificate).
<cert_name>	Enter the name of the certificate.
<tftp_ip>	Enter the IP address of the TFTP server.
<certificate-name_str>	Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
<key_size>	Enter 512, 1024, 1536 or 2048 for the size in bits of the encryption key (RSA key).
<subject>	Enter one of the following pieces of information to identify the FortiAnalyzer unit being certified: • the FortiAnalyzer unit IP address • the fully qualified domain name of the FortiAnalyzer unit • an email address that identifies the FortiAnalyzer unit An IP address or domain name is preferable to an email address.
<country>	Enter the country name, country code, or `null` for none.
<state>	Enter the name of the state or province where the FortiAnalyzer unit is located.
<city>	Enter the name of the city, or town, where the person or organization certifying the FortiAnalyzer unit resides.
<org>	Enter the name of the organization that is requesting the certificate for the FortiAnalyzer unit.
<unit>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiAnalyzer unit.
<email>	Enter a contact e-mail address for the FortiAnalyzer unit.

console

console baudrate

Use this command to get or set the console baudrate.

Syntax

```
execute console baudrate [9600 | 19200 | 38400 | 57600 | 115200]
```

If you do not specify a baudrate, the command returns the current baudrate. Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

```
current baud rate is: 115200
```

date

Get or set the FortiAnalyzer system date.

Syntax

```
execute date [<date_str>]
```

`date_str` has the form `mm/dd/yyyy`, where

- `mm` is the month and can be `1` to `12`
- `dd` is the day of the month and can be `1` to `31`
- `yyyy` is the year and can be `2001` to `2037`

If you do not specify a date, the command returns the current system date.

Dates entered will be validated - `mm` and `dd` require one or two digits, and `yyyy` requires four digits. Entering fewer digits will result in an error.

Example

This example sets the date to 29 September 2015:

```
execute date 9/29/2015
```

device

Use this command to change a device's serial number when changing devices due to a hardware issue, or to change a device's password.

Syntax

To replace a device's password:

```
execute device replace <pw> <name> <pw>
```

To change a device's serial number:

```
execute device replace <sn> <name> <SN>
```

Variable	Description
<pw>	Replace the device password.
<sn>	Replace the device serial number.
<name>	Enter the name of the device.
<pw>	Enter the new password for the new device.
<SN>	Enter the new serial number for the new device.

factory-license

Use this command to enter a factory license key. This command is hidden.

Syntax

```
execute factory-license <key>
```

Variable	Description
<key>	Enter the factory license key.

fgfm

fgfm reclaim-dev-tunnel

Use this command to reclaim a management tunnel.

Syntax

```
execute fgfm reclaim-dev-tunnel <devicename>
```

Variable	Description
<devicename>	Enter the device name. (optional)

fmupdate

Import or export packages using the FTP, SCP, or FTFP servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <remote_file> <ip> <port> <remote_
    path> <user> <password>
```

```
execute fmupdate {ftp | scp | tftp} export <type> <remote_file> <ip> <port> <remote_
    path> <user> <password>
```

Variables	Description
`{ftp | scp | tftp}`	Select `ftp`, `scp`, or `tftp` as the file transfer protocol to use.
`<type>`	Select the type of file to export or import. Options include: `av-ips`, `fct-av`, `url`, `spam`, `license-fgt`, `license-fct`, `custom-url`, and `domp`.
`<remote_file>`	Update manager packet file name on the server or host.
`<ip>`	Enter the FQDN or the IP Address of the server.
`<port>`	Enter the port to connect to on the remote SCP host.
`<remote_path>`	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
`<user>`	Enter the user name to log into the FTP server or SCP host
`<password>`	Enter the password to log into the FTP server or SCP host

format

Format the hard disk on the FortiAnalyzer system. If RAID is configured, change the variable disk-ext4 with `<RAID Level>`.

Syntax

```
execute format {disk | disk-ext4} <RAID Level> <Groups>
```

When you run this command, you will be prompted to confirm the request.

Executing this command will erase all device settings, databases, and log data on the FortiAnalyzer system's hard drive. FortiAnalyzer's IP address, and routing information will be preserved.

Variable	Description
`{disk | disk-ext4}`	Format the hard disk or the ext4 hard disk.
`<RAID Level>`	Select the RAID level to which to format the disk. This option is only available on hardware-based FortiAnalyzer models. For more information on configuring the RAID level, see the *FortiAnalyzer Administration Guide*.

Variable	Description
<Groups>	Enter the group number. This option is only available on hardware-based FortiAnalyzer models configured for RAID 50 or 60. Use * to see a list of the valid groups.

log

Use the following commands to manage device logs:

log device disk_quota	log import
log device logstore	log ips-pkt
log device permissions	log quarantine-files
log dlp-files	

log device disk_quota

Set the log device disk quota.

Syntax

```
execute log device disk_quota <device_id> <value>
```

Variable	Description
<device_id>	Enter the log device ID, or select All for all devices.
<value>	Enter the disk quota value in MB.

Example

The following example sets all log device disk quota values to 200 MB.

```
FAZ1000C # execute log device disk_quota All 200
This will set all devices' disk quota to 200(MB).
Do you want to continue? (y/n)y
Successfully set FG600C3912800438 disk quota to 200 (MB).
Successfully set FG600C3912800830 disk quota to 200 (MB).
Successfully set FGT20C1241584MDL disk quota to 200 (MB).
Successfully set FWF40C3911000061 disk quota to 200 (MB).
Successfully set FE-1002410201202 disk quota to 200 (MB).
Successfully set FGT1001111111111 disk quota to 200 (MB).
Successfully set FGT1001111111112 disk quota to 200 (MB).
Successfully set FG100A2104400006 disk quota to 200 (MB).
Successfully set FG100D3G12809721 disk quota to 200 (MB).
Successfully set FG100D3G12811597 disk quota to 200 (MB).
```

log device logstore

Use this command to view and edit log storage information.

Syntax

```
execute log device logstore clear <device_id>
execute log device logstore list
execute log device logstore move <source_device_id> <destination_device_id>
```

Variable	Description
`clear <device_id>`	Remove leftover log directory.
`list`	List log storage directories.
`move <source_device_id> <destination_device_id>`	Move HA member logs to the HA cluster log directory.

Example

The following example moves all log and archive files from a standalone device ID to the HA cluster device ID.

```
execute log device logstore move 124121 HA123
This will move all logs and archive files from device:124121 to device:HA123.
You may back up all logs of device:124121 before the move.
Please ensure that system has enough extra disk space for the copy of log files from
    both devices.
You may need to rebuild database after moving logs.
Do you want to continue? (y/n)
```

log device permissions

Use this command to view and set log device permissions.

Syntax

```
execute log device permissions <device_id> <permission> {enable | disable}
```

Variable	Description
`<device_id>`	Enter the log device ID, or select All for all devices.
`<permission>`	Select one of the following: • `all`: All permissions • `logs`: Log permission • `content`: Content permission • `quar`: Quarantine permission • `ips`: IPS permission.
`{enable | disable}`	Enable/disable permissions.

Example

The following example enables permissions for all devices.

```
FAZ100C# execute log device permissions All all enable
Set FE-2KB3R09600011 permission all to enable successfully.
Set FWF60C3G12007448 permission all to enable successfully.
Set FG100A2104400006 permission all to enable successfully.
Set FVVM040000008680 permission all to enable successfully.
```

log dlp-files

Use this command to clear DLP log files on a specific log device.

Syntax

```
execute log dlp-files clear <device name> <archive type>
```

Variable	Description
`<device name>`	Enter the name of the log device. Example: FWF40C3911000061
`<archive type>`	Enter the archive type. Select one of: `all`, `email`, `im`, `ftp`, `http`, or `mms`.

log import

Use this command to import log files from another device and replace the device ID on imported logs.

Syntax

```
execute log import <service> <ip> <user-name> <password> <file-name> <device-id>
```

Variable	Description
`<service>`	Enter the transfer protocol. Select one of: `ftp`, `sftp`, `scp`, or `tftp`.
`<ip>`	Enter the server IP address.
`<user-name>`	Enter the username.
`<password>`	Enter the password or '-' for no password. The `<password>` field is not required when `<service>` is `tftp`.
`<file-name>`	The file name (e.g. dir/fgt.alog.log) or directory name (e.g. dir/subdir/).
`<device-id>`	Replace the device ID on imported logs. Enter a device serial number of one of your log devices. For example, FG100A2104400006.

log ips-pkt

Use this command to clear IPS packet logs on a specific log device.

Syntax

```
execute log ips-pkt clear <device name>
```

Variable	Description
<device name>	Enter the name of the log device.

log quarantine-files

Use this command to clear quarantine log files on a specific log device.

Syntax

```
execute log quarantine-files clear <device name>
```

Variable	Description
<device name>	Enter the name of the log device.

log-aggregation

Immediately upload the log to the server.

Syntax

```
execute log-aggregation <id>
```

where `<id>` is the client ID, or `all` for all clients.

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device name> <string>
```

Variable	Description
<device name>	Enter the name of the log device.
<string>	The log file name

lvm

With Logical Volume Manager (LVM), a FortiAnalyzer VM device can have up to twelve total log disks added to an instance. More space can be added by adding another disk and running the LVM extend command.

This command is only available on FortiAnalyzer VM models.

Syntax

```
execute lvm extend <arg ...>
execute lvm info
execute lvm start
```

Variable	Description
`extend`	Extend the LVM logical volume.
`info`	Get system LVM information.
`start`	Start using LVM.
`<arg ...>`	Argument list (0-11). Example disk00.

Example

View LVM information:

```
execute lvm info
   disk01 In use 80.0(GB)
   disk02 Not present
   disk03 Not present
   disk04 Not present
   disk05 Not present
   disk06 Not present
   disk07 Not present
   disk08 Not present
   disk09  Not present
   disk10  Not present
   disk11  Not present
   disk12  Not present
```

ping

Send an Internet Control Message Protocol (ICMP) echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping {<ip> | <hostname>}
```

Variable	Description
<ip>	Enter the IP address of network device to contact.
<hostname>	Enter the DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IP address 192.168.1.23:

```
execute ping 192.168.1.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping6 {<ip> | <hostname>}
```

Variable	Description
<ip>	Enter the IPv6 address of network device to contact.
<hostname>	Enter the DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IP address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute ping6 >8001:0DB8:AC10:FE01:0:0:0:0:
```

raid

This command allows you to add and delete RAID disks.

Syntax

```
execute raid add-disk <disk index>
execute raid delete-disk <disk index>
```

Variable	Description
add-disk <disk index>	Enables you to add a disk and giving it a number.
delete-disk <disk index>	Enables you to delete the selected disk.

Example

The following example shows that disk 5 is added, disk 2 is deleted.

```
execute raid add-disk 5
execute raid delete-disk 2
```

reboot

Restart the FortiAnalyzer system. This command will disconnect all sessions on the FortiAnalyzer system.

Syntax

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n).
```

remove

Use this command to remove reports for a specific device from the FortiAnalyzer system.

Syntax

```
execute remove reports <device-id>
```

reset

Use this command to reset the FortiAnalyzer unit to factory defaults. This command will disconnect all sessions and restart the FortiAnalyzer unit.

Syntax

```
execute reset all-settings
```

Example

```
execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

reset-sqllog-transfer

Use this command to reset SQL logs to the database.

Syntax

```
execute reset-sqllog-transfer <enter>
```

Example

```
execute reset-sqllog-transfer
WARNING: This operation will re-transfer all logs into database.
Do you want to continue? (y/n)
```

restore

Use this command to:

- restore the configuration or database from a file
- change the FortiAnalyzer unit image
- Restore device logs, DLP archives, and reports from specified servers.

This command will disconnect all sessions and restart the FortiAnalyzer unit.

restore all-settings
restore image
restore {logs | logs-only}
restore reports
restore reports-config

restore all-settings

Restore all settings from an FTP, SFTP, or SCP server.

Syntax

```
execute restore all-settings {ftp | sftp} <ip> <string> <username> <password> <crpt_
    password_string> [option1+option2+...]
execute restore all-settings <scp> <ip> <string> <username> <ssh-cert> <crpt_password_
    string> [option1+option2+...]
```

Variable	Description
`all-settings`	Restore all FortiAnalyzer settings from a file on a FTP, SFTP, or SCP server. The new settings replace the existing settings, including administrator accounts and passwords.
`{ftp | sftp}`	Select to restore from an FTP or SFTP server.
`<scp>`	Select to restore from an SCP server.
`<ip>`	Enter the IP address of the server to get the file from.
`<string>`	Enter the file to get from the server. You can enter a path with the filename, if required.
`<username>`	Enter the username to log on to the SCP server.

Variable	Description
<password>	Enter the password for username on the FTP server.
<ssh-cert>	Enter the SSH certificate used for user authentication on the SCP server. This option is not available for restore operations from FTP and SFTP servers.
<crpt_password_string>	Enter the password to protect backup content. Use any for no password. (optional)
[option1+option2+...]	Select whether to keep IP, and routing info on the original unit.

Example

This example shows how to upload a configuration file from a FTP server to the FortiAnalyzer unit. The name of the configuration file on the FTP server is backupconfig. The IP address of the FTP server is 192.168.1.23. The user is admin with a password of mypassword. The configuration file is located in the /usr/local/backups/ directory on the FTP server.

```
execute restore all-settings FTP 192.168.1.23 /usr/local/backups/backupconfig admin
    mypassword
```

restore image

Use this command to restore an image to the FortiAnalyzer.

Syntax

```
execute restore image ftp <filepath> <ip> <username> <password>
execute restore image tftp <string> <ip>
```

Variable	Description
image	Upload a firmware image from a TFTP server to the FortiAnalyzer unit. The FortiAnalyzer unit reboots, loading the new firmware.
<filepath>	Enter the file path on the FTP server.
<string>	Enter the image file name on the TFTP server.
<ip>	Enter the IP address of the server to get the file from.
<username>	Enter the username to log on to the server. This option is not available for restore operations from FTP servers.
<password>	Enter the password for username on the FTP server. This option is not available for restore operations from TFTP servers.

restore {logs | logs-only}

Use this command to restore logs and DLP archives from a specified server.

Syntax

```
execute restore logs <device name> <service> <ip> <user name> <password> <directory>
execute restore logs-only <device name> <service> <ip> <user name> <password>
    <directory>
```

Variable	Description
`logs`	Restore device logs and DLP archives from a specified server.
`logs-only`	Restore device logs from a specified server.
`<device name>`	Device name or names, separated by commas, or `all` for all devices. For example: `FWF40C3911000061`.
`<service>`	Select the transfer protocol. Select one of FTP, SFTP, or SCP.
`<ip>`	Enter the IP address of the server to get the file from.
`<user name>`	Enter the username to log on to the SCP server. This option is not available for restore operations from FTP servers.
`<password>`	Enter the password for username on the FTP server. This option is not available for restore operations from TFTP servers.
`<directory>`	Enter the directory on the server.

restore reports

Use this command to restore reports from a specified server.

Syntax

```
execute restore reports {<report name> | all | <report name pattern} <service> <ip>
    <user name> <password> <directory>
```

Variable	Description
`reports`	Restore reports from a specified server.

`{<report name> | all | <report name pattern}`	Backup specific reports, all reports, or reports with names containing given pattern.
	• A '?' matches any single character.
	• A '*' matches any string, including the empty string, e.g.:
	  • foo: for exact match
	  • *foo: for report names ending with foo
	  • foo*: for report names starting with foo
	  • *foo*: for report names containing foo substring

`<service>`	Select the transfer protocol. Select one of FTP, SFTP, or SCP.

Variable	Description
<ip>	Enter the IP address of the server to get the file from.
<user name>	Enter the username to log on to the SCP server. This option is not available for restore operations from FTP servers.
<password>	Enter the password for username on the FTP server. This option is not available for restore operations from TFTP servers.
<directory>	Enter the directory on the server.

restore reports-config

Use this command to restore a report configuration from a specified server.

Syntax

```
execute restore <reports-config> {<adom_name> | all]} <service> <ip> <user name>
    <password> <directory>
```

Variable	Description
{<adom_name> | all]}	Select to backup a specific ADOM or all ADOMs.
<service>	Select the transfer protocol. Select one of: `ftp, sftp, scp`.
<ip>	Enter the server IP address
<user name>	Enter the username on the server
<password>	Enter the password, or '-' for none.
<directory>	Enter the directory on the server, or press `<Enter>` for none.

Example

```
This command restores all reports config from a specified server which were backed up
    previously.
All reports schedule will be cleared after restoration!
Do you want to continue? (y/n)
```

shutdown

Shut down the FortiAnalyzer system. This command will disconnect all sessions.

Syntax

```
execute shutdown
```

Example

```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```

sql-local

Use this command to remove the SQL database and logs from the FortiAnalyzer system and to rebuild the database and devices.

sql-local rebuild-db
sql-local remove-db
sql-local remove-logtype

When rebuilding the SQL database, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

sql-local rebuild-db

Use this command to rebuild the entire local SQL database.

Syntax

```
execute sql-local <rebuild-db>
```

sql-local remove-db

Use this command to remove an entire local SQL database.

Syntax

```
execute sql-local remove-db
```

sql-local remove-logtype

Use this command to remove all log entries of the designated log type.

Syntax

```
execute sql-local remove-logtype <log type>
```

Variable	Description
`<log type>`	Enter the log type from available log types, for example: `app-ctrl`

Example

```
execute sql-local remove-logtype app-ctrl
All SQL logs with log type 'app-ctrl' will be erased!
Do you want to continue? (y/n)
```

sql-query-dataset

Use this command to execute a SQL dataset against the FortiAnalyzer system.

Syntax

```
execute sql-query-dataset <adom> <dataset-name> <device/group name> <faz/dev> <start-
    time> <end-time>
```

Variable	Description
`<adom>`	Enter the name of the ADOM.
`<dataset-name>`	Enter the dataset name.
`<device/group name>`	Enter the name of the device, for example: `FWF40C3911000061`
`<faz/dev>`	Enter the name of the FortiAnalyzer.
`<start-time>`	Enter the log start time.
`<end-time>`	Enter the log end time.

Example

```
execute sql-query-dataset Top-App-By-Bandwidth
```

sql-query-generic

Use this command to execute a SQL statement against the FortiAnalyzer system.

Syntax

```
execute sql-query-generic <string>
```

Variable	Description
`<string>`	Enter the SQL statement to run.

sql-report

Use these commands to import and display language translation files and run a SQL report schedule once against the FortiAnalyzer system.

Syntax

```
execute sql-report hcache-check <adom> <schedule-name> <start-time> <end-time>
execute sql-report import-lang <language-name> <service> <ip> <argument 1> <argument 2>
    <argument 3>
execute sql-report list <adom> [days-range] [layout-name]
execute sql-report list-lang
execute sql-report list-schedule <adom>
execute sql-report run <adom> <schedule-name> <start-time> <end-time>
execute sql-report view <data-type> <adom> <report-name>
```

Variable	Description
`<adom>`	Specify the ADOM name.
`<schedule-name>`	Select one of the available SQL report schedule names.
`<start-time>`	Start date and time <"HH:MM yyyy/mm/dd"> of the report schedule.
`<end-time>`	End date and time <"HH:MM yyyy/mm/dd"> of the report schedule.
`<language-name>`	Enter the new language name to import a new language translation file.
`<service>`	Transfer protocol [ftp|sftp|scp|tftp]
`<ip>`	Server IP address.
`<argument 1>`	For FTP, SFTP, or SCP, enter a user name. For TFTP, enter a file name.
`<argument 2>`	For FTP, SFTP, or SCP, enter a password or '-'. For TFTP, press <enter>.
`<argument 3>`	Enter a filename and press <enter>.
`[days-range]`	The recent n days to list reports, from 1 to 99.
`[layout-name]`	One of the available SQL report layout names.
`<data-type>`	The data type to view. Must be `report-data`.
`<report-name>`	The name of the report to view.

Example

The following command runs a specific report (6) against an ADOM (Test).

```
execute sql-report run root Test 6
   Number of threads is invalid or exceeds the limit (6), use default value (2).
   layout_num:1
```

```
start [0] get layout-id:6.
start report_process, layout-id:6, layout title:Doc.
device list:All_FortiGates.
reports num:1.
device list[0].FGT20C1241584MDL[root].
device list[1].FWF40C3911000061[root].
device list[2].FG100D3G12809721[root].
device list[3].FG100D3G12809721[vdom1].
device list[4].FG100D3G12811597[root].
device list[5].FG100D3G12811597[vdom1].
> running (D-6_t6-2013-03-11-1141) ...
> rendering (D-6_t6-2013-03-11-1141) (en) ...
sql_rpt_render_dir : start
pdfv2_rpt_init:774 ---------PDF report init.----Language: en---------
set_msg_lvl:108 current pdfv2 message level: 1
pdfv2_rpt_page_begin:999 info: create new page 0
pdfv2_rpt_page_begin:999 info: create new page 1
pdfv2_rpt_page_begin:999 info: create new page 2
pdfv2_rpt_section:1254 info: create outline (Appendix A) level 1
pdfv2_rpt_page_begin:999 info: create new page 3
pdfv2_rpt_page_begin:999 info: create new page 4
pdfv2_rpt_section:1254 info: create outline (Appendix B) level 1
pdfv2_rpt_clean:683 Saved PDF report to /Storage/Reports/ADOMs/root/2013_03_11/D-6_
    t6-2013-03-11-1141/FortiAnalyzer_Report.pdf
Report [D-6_t6-2013-03-11-1141] finished at Mon (1) 2013-03-11 11:41:24.
```

ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination> <username>
```

Variable	Description
`<destination>`	Enter the IP or FQ DNS resolvable hostname of the system you are connecting to.
`<username>`	Enter the user name to use to log on to the remote system.

To leave the SSH session type `exit`. To confirm you are connected or disconnected from the SSH session, verify that the command prompt has changed.

ssh-known-hosts

Use this command to remove all known SSH hosts.

Syntax

```
execute ssh-known-hosts remove-all
execute ssh-known-hosts remove-host <host/ip>
```

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

`time_str` has the form `hh:mm:ss`, where

- `hh` is the hour and can be `00` to `23`
- `mm` is the minutes and can be `00` to `59`
- `ss` is the seconds and can be `00` to `59`

All parts of the time are required. Single digits are allowed for each of `hh`, `mm`, and `ss`. If you do not specify a time, the command returns the current system time.

```
execute time <enter>
current time is: 12:54:22
```

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

top

Use this command to view the processes running on the FortiAnalyzer system.

Syntax

```
execute top
```

Help menu

Command	Description
`Z,B`	Global: 'Z' change color mappings; 'B' disable/enable bold
`l,t,m`	Toggle Summaries: 'l' load average; 't' task/cpu statistics; 'm' memory information
`1,I`	Toggle SMP view: '1' single/separate states; 'I' Irix/Solaris mode
`f,o`	Fields/Columns: 'f' add or remove; 'o' change display order
`F or O`	Select the sort field
`<,>`	Move sort field: '<' next column left; '>' next column right

Command	Description
R,H	Toggle: 'R' normal/reverse sort; 'H' show threads
c,i,S	Toggle: 'c' command name/line; 'i' idle tasks; 'S' cumulative time
x,y	Toggle highlights: 'x' sort field; 'y' running tasks
z,b	Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
u	Show specific user only
n or #	Set maximum tasks displayed
k,r	Manipulate tasks: 'k' kill; 'r' renice
d or s	Set update interval
W	Write configuration file
q	Quit

Example

The `execute top` command displays the following information:

```
top_bin - 13:14: 18 up 21:17, 0 users, load average: 0.02, 0.05, 0.05
Tasks: 152 total, 1 running, 151 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.8%us, 0.2%sy, 0.0%ni, 99.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 3080612k total, 1478800k used, 1601812k free, 95016k buffers
Swap: 2076536k total, 0k used, 2076536k free, 782268k cached
H
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 3943 root 20 0 210m 181m 11m S 0 6.0 0:43.42 gui control
 4022 root 20 0 11072 4504 1972 S 0 0.1 1:30.95 udm_statd
 1 root 20 0 194m 167m 5104 S 0 5.6 0:14.69 initXXXXXXXXXXXX
 2 root 20 0 0 0 0 S 0 0.0 0:00.00 kthreadd
 3 root 20 0 0 0 0 S 0 0.0 0:00.13 ksoftirqd/0
 4 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/0:0
 6 root RT 0 0 0 0 S 0 0.0 0:00.01 migration/0
 7 root RT 0 0 0 0 S 0 0.0 0:00.03 migration/1
 8 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/1:0
 9 root 20 0 0 0 0 S 0 0.0 0:00.13 ksoftirqd/1
 10 root 20 0 0 0 0 S 0 0.0 0:02.80 kworker/0:1
 11 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/2
 12 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/2:0
 13 root 20 0 0 0 0 S 0 0.0 0:00.08 ksoftirqd/2
 14 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/3
 15 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/3:0
```

traceroute

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute <host>
```

Variable	Description
<host>	Enter the IPv4 address or hostname of network device.

Example

This example shows how trace the route to a host with the IP address 172.18.4.95:

```
execute traceroute 172.18.4.95
traceroute to 172.18.4.95 (172.18.4.95), 32 hops max, 72 byte packets
1 172.18.4.95 0 ms 0 ms 0 ms
2 172.18.4.95 0 ms 0 ms 0 ms
```

traceroute6

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute6 <host>
```

The following table lists command variables, descriptions, and default values where applicable.

Variable	Description
<host>	Enter the IPv6 address or hostname of network device.

Example

This example shows how trace the route to a host with the IPv6 address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute traceroute6 8001:0DB8:AC10:FE01:0:0:0:0
```

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.

FortiAnalyzer commands and variables are case sensitive.

This chapter contains following sections:

auto-delete	fmupdate	sql
cdb check	fortilogd	system
debug	hardware	test
dlp-archives	log device	upload
dvm	pm2	vpn
fgfm	report	
fmnetwork	sniffer	

auto-delete

Use this command to view and configure auto-deletion settings.

Syntax

```
diagnose auto-delete dlp-files {list | delete-now}
diagnose auto-delete log-files {list | delete-now}
diagnose auto-delete quar-files {list | delete-now}
diagnose auto-delete report-files {list | delete-now}
```

Variable	Description
`dlp-files {list | delete-now}`	View and configure auto-deletion of DLP files.
`log-files {list | delete-now}`	View and configure auto-deletion of log files.
`quar-files {list | delete-now}`	View and configure auto-deletion of quarantined files.
`report-files {list | delete-now}`	View and configure auto-deletion of report files.

cdb check

Use this command to check the object configuration database integrity and the global policy assignment table.

Syntax

```
diagnose cdb check objcfg-integrity
diagnose cdb check policy-assignment
diagnose cdb check reference-integrity
diagnose cdb check update-devinfo <item> [new-value] [0|1] [model-name]
```

Variable	Description
`objcfg-integrity`	Check object config database integrity.
`policy-assignment`	Check the global policy assignment table.
`reference-integrity`	Check the ADOM reference table integrity.

`update-devinfo`	Update device information by directly changing the database.
	• `<item>`: Device info item.
	• `[new-value]`: Item new value (Default sump summary only).
	• `[0|1]`: Choose one of:
	  • `0`: Only update empty value (default).
	  • `1`: Always update
	• `[model-name]`: Only update on model name. Default: all models.

debug

Use the following commands to debug the FortiAnalyzer.

debug application
debug cli
debug console
debug crashlog
debug disable
debug enable
debug info
debug reset
debug service
debug sysinfo
debug sysinfo-log
debug sysinfo-log-backup
debug sysinfo-log-list
debug timestamp
debug vminfo

debug application

Use this command to set the debug levels for the FortiAnalyzer applications.

Syntax

```
diagnose debug application alertmail <integer>
diagnose debug application curl <integer>
diagnose debug application ddmd <integer> <devicename>
diagnose debug application depmanager <integer>
diagnose debuf application dmworker <integer>
diagnose debug application dmapi <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fgdsvr <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmd <integer> <devicename>
diagnose debug application fnbam <integer>
diagnose debug application fortilogd <integer>
diagnose debug application fortimanagerws <integer>
diagnose debug application gui <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application log-aggregate <integer>
diagnose debug application logd <integer>
diagnose debug application logfiled <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application oftpd <integer> <IP/deviceSerial/deviceName>
diagnose debug application ptmgr <integer>
diagnose debug application ptsessionmgr <integer>
diagnose debug application securityconsole <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqlplugind <integer>
diagnose debug application sqlrptcached <integer>
diagnose debug application srchd <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <integer>
diagnose debug application storaged <integer>
diagnose debug application uploadd <integer>
```

Variable	Description	Default
`alertmail <integer>`	Set the debug level of the alert email daemon.	0
`curl <integer>`	This command is not in use.	
`ddmd <integer> <devicename>`	Set the debug level of the dynamic data monitor.	0
`depmanager <integer>`	Set the debug level of the deployment manager.	0
`dmworker <integer>`	Set the debug level of the deployment manager worked.	

Variable	Description	Default
`dmapi <integer>`	Set the debug level of the `dmapi` daemon.	0
`fazcfgd <integer>`	Set the debug level of the `fazcfgd` daemon.	0
`fazsvcd <integer>`	Set the debug level of the `fazsvcd` daemon.	0
`fgdsvr <integer>`	Set the debug level of the FortiGuard query daemon.	0
`fgdupd <integer>`	Set the debug level of the FortiGuard update daemon.	0
`fgfmd <integer> <devicename>`	Set the debug level of `FGFM` daemon.	0
`fnbam <integer>`	Set the debug level of the Fortinet authentication module.	0
`fortilogd <integer>`	Set the debug level of the `fortilogd` daemon.	0
`fortimanagerws <integer>`	Set the debug level of the FortiAnalyzer Web Service.	0
`gui <integer>`	Set the debug level of the GUI.	0
`ipsec <integer>`	Set the debug level of the `IPsec` daemon.	0
`localmod <integer>`	Set the debug level of the `localmod` daemon.	0
`log-aggregate <integer>`	Set the debug level of the log aggregate daemon.	0
`logd <integer>`	Set the debug level of the log daemon.	0
`logfiled <integer>`	Set the debug level of the `logfilled` daemon.	0
`lrm <integer>`	Set the debug level of the Log and Report Manager.	0
`ntpd <integer>`	Set the debug level of the Network Time Protocol (NTP) daemon.	0
`oftpd <integer> <IP/deviceSerial/deviceName>`	Set the debug level of the `oftpd` daemon.	0

Variable	Description	Default
`ptmgr <integer>`	Set the debug level of the Portal Manager.	0
`ptsessionmgr <integer>`	Set the debug level of the Portal Session Manager.	0
`securityconsole <integer>`	Set the debug level of the security console daemon.	0
`snmpd <integer>`	Set the debug level of the SNMP daemon from 0-8.	0
`sql_dashboard_rpt <integer>`	Set the debug level of the SQL dashboard report daemon.	0
`sql-integration <integer>`	Set the debug level of SQL applications.	0
`sqlplugind <integer>`	Set the debug level of the SQL plugin daemon.	0
`sqlrptcached <integer>`	Set the debug level of the SQL report caching daemon.	0
`srchd <integer>`	Set the debug level of the `SRCHD`.	0
`ssh <integer>`	Set the debug level of SSH protocol transactions.	0
`sshd <integer>`	Set the debug level of the SSH daemon.	
`storaged <integer>`	Set the debug level of communication with java clients.	0
`uploadd <integer>`	Set the debug level of the upload daemon.	0

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description	Default
`<integer>`	Set the debug level of the CLI from 0-8.	3

debug console

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug console {enable | disable}
```

Variable	Description
`{enable | disable}`	Enable/disable console debugging.

debug crashlog

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug crashlog clear
```

Variable	Description
`clear`	Clear the crash log.

debug disable

Use this command to disable debugging.

Syntax

```
diagnose debug disable
```

debug enable

Use this command to enable debugging.

Syntax

```
diagnose debug enable
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

Variable	Description
`info`	Show active debug level settings.

debug reset

Use this command to reset debug level settings.

Syntax

```
diagnose debug reset
```

debug service

Use this command to debug service daemons.

Syntax

```
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service fazconf <integer>
diagnose debug service main <integer>
daignose debug service sys <integer>
diagnose debug service task <integer>
```

Variable	Description
`<integer>`	Debug level.

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

Variable	Description
`sysinfo`	Show system information.

debug sysinfo-log

Use this command to generate one system info log file every 2 minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

Variable	Description
`sysinfo-log {on | off}`	Enable to generate one system info log file every 2 minutes.

debug sysinfo-log-backup

Use this command to backup all sysinfo log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <ip> <string> <username> <password>
```

Variable	Description
sysinfo-log-backup	Show system information.
<ip>	Enter the FTP server IP address.
<string>	Enter the path/filename to save the log to the FTP server.
<username>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug sysinfo-log-list

Use this command to display system info elogs.

Syntax

```
diagnose debug sysinfo
```

Variable	Description
sysinfo	Show system information.

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

Variable	Description
{enable | disable}	Enable/disable debug timestamp.

debug vminfo

Use this command to show FortiAnalyzer VM license information.

Syntax

```
diagnose debug vminfo
```

dlp-archives

Use the following commands for DLP archive related settings.

dlp-archives quar-cache
dlp-archives statistics
dlp-archives rebuild-quar-db
dlp-archives status

dlp-archives quar-cache

Use this command to view the quarantine cache.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
```

Variable	Description
`list-all-process`	List all processes using the quarantine cache.

dlp-archives rebuild-quar-db

Use this command to rebuild the quarantine cache database.

Syntax

```
diagnose dlp-archives rebuild-quar-db
```

dlp-archives statistics

Use this command to view and flush the quarantined and DLP archived file statistics.

Syntax

```
diagnose dlp-archives statistics <flush>
diagnose dlp-archives statistics <show>
```

Variable	Description
`<flush>`	Flush the quarantined and DLP archived file statistics.
`<show>`	Display the quarantined and DLP archived file statistics.

dlp-archives status

Use this command to view the DLP archive status.

Syntax

```
diagnose dlp-archives staus
```

dvm

Use the following commands for DVM related settings.

dvm adom	dvm device	dvm proc
dvm chassis	dvm device-tree-update	dvm task
dvm check-integrity	dvm group	dvm transaction-flag
dvm debug	dvm lock	

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list
```

Variable	Description
`list`	List the ADOMs configured on the FortiAnalyzer.

dvm chassis

Use this command to list chassis.

Syntax

```
diagnose dvm chassis list
```

Variable	Description
`list`	List chassis.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

dvm debug

Use this command to enable or disable debug channels.

Syntax

```
diagnose dvm debug enable <channel>
```

```
diagnose dvm debug disable <channel>
```

Variable	Description
enable <channel>	Select to enable debug channel including: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, monitor.
disable <channel>	Select to disable debug channel including: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, monitor.

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device dynobj <device> <cli>
diagnose dvm device list <device> <vdom>
diagnose dvm device delete <adom> <device>
```

Variable	Description
dynobj <device> <cli>	List dynamic objects on this device. For <device>, enter the name of the displayed in the diagnose dvm device list command. Optionally, use 1 for <cli> to display the CLI configuration.
list <device> <vdom>	List devices and VDOMs that are currently managed by the FortiAnalyzer. This command displays the following information: type, OID, SN, HA, IP, name, ADOM, and firmware.
delete <adom> <device>	Delete devices.

dvm device-tree-update

Use this command to enable or disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

Variable	Description
{enable | disable}	Enable/disable DVM device tree updates.

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

Variable	Description
`list`	List groups.

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

dvm proc

Use this command to list DVM processes.

Syntax

```
diagnose dvm proc list
```

Variable	Description
`list`	List DVM process (dvmcmd) information.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
`list <adom> <type>`	List the task database. • ADOM filter options: `all`, `global`, `adom` • Type filter options: `all`, `type`
`repair`	Repair the task database while preserving existing data where possible. The FortiAnalyzer will reboot after the repairs.
`reset`	Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiAnalyzer will reboot after the reset.

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag {abort | debug | none}
```

Variable	Description
`transaction-flag {abort | debug | none}`	DVM transaction flag options.

fgfm

Use this command to get installation object lists.

Syntax

```
diagnose fgfm object-list
```

Variable	Description
`object-list`	Get object lists.

fmnetwork

Use the following commands for network related settings:

- fmnetwork arp
- fmnetwork interface
- fmnetwork netstat

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <ip>
diagnose fmnetwork arp list
```

Variable	Description
`del <intf-name> <ip>`	Delete an ARP entry.
`list`	List ARP entries.

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <portX>
diagnose fmnetwork interface list <portx>
```

Variable	Description
`detail <portX>`	View a specific interface's details. This command displays the following information: status, speed, and duplex.
`list <portx>`	List all interface details, or enter <portx> to display information for a specific interface.

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp [-r]
```

Variable	Description
`list [-r]`	List all connections, or use -r to list only resolved IP addresses.
`tcp [-r]`	List all TCP connections, or use -r to list only resolved IP addresses.
`udp [-r]`	List all UDP connections, or use -r to list only resolved IP addresses.

fmupdate

Use these commands to diagnose update services.

Syntax

```
diagnose fmupdate add-device <serial> <ip> <firmware> <build>
diagnose fmupdate deldevice {fct | fds | fgd | fgc} <serial> <uid>
diagnose fmupdate dellog
diagnose fmupdate fct-configure
diagnose fmupdate fct-dbcontract
diagnose fmupdate fct-delserverlist
diagnose fmupdate fct-getobject
diagnose fmupdate fct-serverlist
diagnose fmupdate fct-update-status
diagnose fmupdate fct-updatenow
diagnose fmupdate fds-configure
```

```
diagnose fmupdate fds-dbcontract
diagnose fmupdate fds-delserverlist
diagnose fmupdate fds-dump-breg
diagnose fmupdate fds-dump-srul
diagnose fmupdate fds-get-downstream-device
diagnose fmupdate fds-getobject
diagnose fmupdate fds-serverlist
diagnose fmupdate fds-service-info
diagnose fmupdate fds-update-status
diagnose fmupdate fds-updatenow
diagnose fmupdate fgd-updatenow
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} {add | del | required}
diagnose fmupdate getdevice {fct | fds | fgd | fgc} <serial>
diagnose fmupdate service-restart <string>
diagnose fmupdate show-bandwidth <type> <time_period>
diagnose fmupdate show-dev-obj <string>
diagnose fmupdate view-linkd-log <string>
diagnose fmupdate vm-license
```

Keywords and Variables	Description
`add-device <serial> <ip> <firmware> <build>`	Add an unregistered device. The build number is optional.
`deldevice {fct | fds | fgd | fgc} <serial> <uid>`	Delete a device. The UID applies only to FortiClient devices.
`dellog`	Delete log for FDS/FortiGuard update events.
`fct-configure`	Dump the FortiClient running configuration.
`fct-dbcontract`	Dump the FortiClient subscriber contract.
`fct-delserverlist`	Dump the FortiClient server list file fdni.dat.
`fct-getobject`	Get the version of all FortiClient objects.
`fct-serverlist`	Dump the FortiClient server list.
`fct-update-status`	Display the FortiClient update status.
`fct-updatenow`	Update the FortiClient AV/IPS immediately.
`fds-configure`	Dump the FortiDNS running configuration.
`fds-dbcontract`	Dump the FortiDNS subscriber contract

Keywords and Variables	Description
`fds-delserverlist`	Delete the FortiDNS server list file fdni.dat.
`fds-dump-breg`	Dump the FortiDNS beta serial numbers.
`fds-dump-srul`	Dump the FortiDNS select filtering rules.
`fds-get-downstream-device`	Get information of all downstream FortiGate AV-IPS devices.
`fds-getobject`	Get the version of all FortiGate objects.
`fds-serverlist`	Dump the FortiDNS server list.
`fds-service-info`	Display FortiDNS service information.
`fds-update-status`	Display the FortiDNS update status.
`fds-updatenow`	Update the FortiGate AV/IPS immediately.
`fgd-updatenow`	Update the FortiGate web filter / antispam immediately.
`fgt-del-statistics`	Remove all statistics (AV/IPS and web filter / antispam). This command requires a reboot.
`fgt-del-um-db`	remove UM and UM-GUI databases.This command requires a reboot.
`fmg-statistic-info`	Display statistic information for FortiAnalyzer and Java Client.
`fortitoken {seriallist | add | del} {add | del | required}`	FortiToken related operations.
`getdevice {fct | fds | fgd | fgc} <serial>`	Get device information.
`service-restart <string>`	Restart the `linkd` service. The string value includes the type [fct|fds|fgd|fgc].
`show-bandwidth <type> <time_period>`	Display the download bandwidth. The type value includes [fct|fds|fgd|fgc]. The time_period value includes [1h|6h|12h|24|7d|30d>.
`show-dev-obj <string>`	Display objects version of device. Serial number of the device. (optional)

Keywords and Variables	Description
view-linkd-log <string>	View the linkd log file. The string value includes the type [fct|fds|fgd|fgc].
vm-license	Dump the FortiGate VM license.

Example

To view antispam server statistics for the past seven days, enter the following:

```
diagnose fmupdate fgd-asserver_stat 7d
```

The command returns information like this:

```
Server Statistics
Total Spam Look-ups: 47
Total # Spam: 21(45%)
Total # Non-spam:26(55%)
Estimated bandwidth usage:17MB
```

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd msgrate
diagnose fortilogd msgrate-device
diagnose fortilogd msgrate-total
diagnose fortilogd msgrate-type
diagnose fortilogd msgstat <flush>
diagnose fortilogd lograte
diagnose fortilogd status
```

Variable	Description
msgrate	Display log message rate.
msgrate-device	Display log message rate devices.
msgrate-total	Display log message rate totals.
msgrate-type	Display log message rate types.
msgstat <flush>	Display or flush log message statuses.
lograte	Display the log rate.
status	Running status.

Example

This is an example of the output of `diagnose fortilogd status`:

```
fortilogd is starting
config socket OK
cmdb socket OK
cmdb register log.device OK
cmdb register log.settings OK
log socket OK
reliable log socket OK
```

hardware

Use this command to view hardware information. This command provides comprehensive system information including: CPU, memory, disk, and RAID information.

Syntax

```
diagnose hardware info
```

log device

Use this command to view device log usage.

Syntax

```
diagnose log device
```

pm2

Use these commands to check the integrity of the database.

Syntax

```
diagnose pm2 check-integrity db-category {all | adom | device |global | ips}
diagnose pm2 print <log-type>
```

Variable	Description
`db-category {all | adom | device |global | ips}`	Check the integrity of the database. Multiple database categories can be selected.
`<log-type>`	Print the database log messages.

report

Use this command to check the SQL database.

Syntax

```
diagnose report clean
diagnose report status {pending | running}
```

Variable	Description
`clean`	Cleanup the SQL report queue.
`status {pending | running}`	Check status information on pending and running reports list.

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiAnalyzer units have a built-in sniffer. Packet capture on FortiAnalyzer units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing `Control + C`, or until it reaches the number of packets that you have specified to capture.

Packet capture can be very resource intensive. To minimize the performance impact on your FortiAnalyzer unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface_name> <filter_str> <verbose> <count>
```

Variable	Description	Default
`<interface_name>`	Type the name of a network interface whose packets you want to capture, such as `port1`, or type `any` to capture packets on all network interfaces.	No default

Variable	Description	Default
`<filter_str>`	Type either `none` to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as `'tcp port 25'`. Surround the filter string in quotes. The filter uses the following syntax: `'[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or] [[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]'` To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source, and which is the destination. For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter: `'udp and port 1812 and src host 1.example.com and dst \( 2.example.com or 2.example.com \)'`	none
`<verbose>`	Type one of the following numbers indicating the depth of packet headers and payloads to capture: • `1`: header only • `2`: IP header and payload • `3`: Ethernet header and payload For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (`3`).	1
`<count>`	Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press Control + C.	

Example

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named port1. The capture uses a low level of verbosity (indicated by `1`).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by `1`). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Control + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and tcp port 80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by `3`).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Control + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer # diag sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 ..........)...E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f........
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or............
0x0040 86bb 0000 0000 0103 0303 ..........
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is usually preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark (http://www.wireshark.org/).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY
- a plain text editor such as Notepad

- a Perl interpreter
- network protocol analyzer software such as Wireshark

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Type the packet capture command, such as:
   ```
   diagnose sniffer packet port1 'tcp port 541' 3 100
   ```
   but do not press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.
   A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session* > *Logging.*
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the .log file extension.)
8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiAnalyzer unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `Control + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.
13. Delete the first and last lines, which look like this:
    ```
    =~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 7/14/2016.07.25 11:34:40 =~=~=~=~=~=~=~=~=~=~=~=~=~=
    Fortinet-2000 #
    ```
    These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.
14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
    You can convert the plain text file to a format (.pcap) recognizable by Wireshark using the fgt2eth.pl Perl script. To download fgt2eth.pl, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

> The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

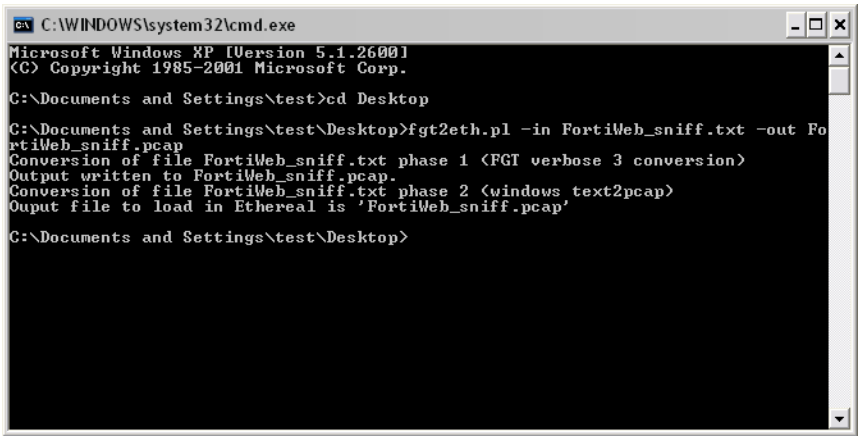
To use fgt2eth.pl, open a command prompt, then enter a command such as the following:

> Methods to open a command prompt vary by operating system.
> On Windows XP, go to *Start* > *Run* and enter `cmd`
> On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved.



15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

    For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

sql

Use this command to diagnose the SQL database.

Syntax

```
diagnose sql config debug-filter set <string>
diagnose sql config debug-filter test <string>
diagnose sql config deferred-index-timespan set <string>
diagnose sql config top-dev det [{log-thres | num-max}] <integer>
diagnose sql gui-rpt-shm <list-all>
diagnose sql gui-rpt-shm clear <num>
diagnose sql process list full
diagnose sql process kill <pid>d
diagnose sql rebuild-report-hcache <start-time> <end-time>
diagnose sql remove hcache <device-id>
diagnose sql remove query-cache
diagnose sql remove tmp-table
diagnose sql show {db-size | hcache-size}
diagnose sql show log-filters
diagnose sql show log-stfile <device-id>
diagnose sql status {run_sql_rpt | sql_hcache_chk | sqlplugind | sqlreportd | rebuild-
    db}
diagnose sql upload <ftp host> <ftp dir> <ftp user name> <ftp password>
```

Variable	Description
`config debug-filter set <string>`	Set the sqlplugin debug filter.
`config debug-filter test <string>`	Test the sqlplugin debug filter
`config deferred-index-timespan set <string>`	Set the time span for the deferred index.
`config top-dev det [{log-thres | num-max}] <integer>`	Set the SQL plugin top devices settings including: • `log-thres`: Log threshold of top devices. • `num-max`: Maximum number of top devices. Select a number between 0 and 1000.
`gui-rpt-shm <list-all>`	List all asynchronous GUI report shared memory slot information.
`gui-rpt-shm clear <num>`	Clear asynchronous GUI report shared memory slot information.
`process list full`	List running query processes.
`process kill <pid>`	Kill a running query.
`rebuild-report-hcache <start-time> <end-time>`	Rebuild `hcache` for report. Enter the start time/end time in the format "`yyyy-mm-dd hh:mm:ss`".
`remove hcache <device-id>`	Remove the `hcache` tables created for the SQL report.
`remove query-cache`	Remove the SQL query cache for log search.
`remove tmp-table`	Remove the SQL database temporary tables.
`show {db-size | hcache-size}`	Show the database or hcache size.
`show log-filters`	Show log view searching filters.
`show log-stfile <device-id>`	Show the log status file.
`status {run_sql_rpt | sql_hcache_chk | sqlplugind | sqlreportd | rebuild-db}`	Show run_sql_rpt, sql_hcache_chk, sqlplugind, or sqlreportd status.
`upload <ftp host> <ftp dir> <ftp user name> <ftp password>`	Upload sqlplugind messages / pgsvr logs via FTP.

system

Use the following commands for system related settings.

system admin-session	system fsck	system process
system disk	system geoip	system raid
system export	system ntp	system route
system flash	system print	system route6

system admin-session

Use this command to view login session information.

Syntax

```
diagnose system admin-session list
diagnose system admin-session status
diagnose system admin-session kill
```

Variable	Description
`list`	List login sessions.
`status`	Show the current session.
`kill`	Kill a current session.

Example

This is an example of the output from `diagnose system admin-session status`:

```
session_id: 31521 (seq: 4)
username: admin
admin template: admin
from: jsconsole(10.2.0.250)
profile: Super_User (type 3)
adom: root
session length: 198 (seconds)
```

system disk

Use this command to view disk diagnostic information.

Syntax

```
diagnose system disk attributes
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
```

```
diagnose system disk errors
```

Variable	Description
attributes	Show vendor specific SMART attributes.
disable	Disable SMART support.
enable	Enable SMART support.
health	Show the SMART health status.
info	Show the SMART information.
errors	Show the SMART error logs.

system export

Use this command to export logs.

Syntax

```
diagnose system export crashlog <server> <user> <password> <directory> <filename>
diagnose system export dminstallog <devid> <server> <user> <password> <directory>
    <filename>
diagnose system export fmwslog {sftp | ftp} <type> <(s)ftp server> <username>
    <password> <directory> <filename>
diagnose system export umlog {sftp | ftp} <type> <(s)ftp server> <username> <password>
    <directory> <filename>
diagnose system export upgradelog <ftp server> <usernmae> <password> <directory>
    <filename>
```

Variable	Description
crashlog <server> <user> <password> <directory> <filename>	Export the crash log.
dminstallog <devid> <server> <user> <password> <directory> <filename>	Export deployment manager install log.

Variable	Description
`fmwslog {sftp | ftp} <type> <(s)ftp server> <username> <password> <directory> <filename>`	Export the FortiAnalyzer Web Service log files to an SFTP or FTP server. The type options are: `SENT`, `RECV`, `TEST`.
`umlog {sftp | ftp} <type> <(s)ftp server> <username> <password> <directory> <filename>`	Export the update manager and firmware manager log files. The `type` option are: `fdslinkd`, `fctlinkd`, `fgdlinkd`, `usvr`, `update`, `service`, `misc`, `umad`, and `fwmlinkd`.
`upgradelog <ftp server> <usernmae> <password> <directory> <filename>`	Export the upgrade error log.

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

Variable	Description
`list`	List flash images. This command displays the following information: image name, version, total size (KB), used (KB), percent used, boot image, and running image.

system fsck

Use this command to check and repair the file system, and to reset the disk mount count.

Syntax

```
diagnose system fsck harddisk
diagnose system fsck reset-mount-count
```

Variable	Description
`harddisk`	Check and repair the file system, then reboot the system.
`reset-mount-count`	Reset the mount-count of the disk.

system geoip

Use this command to list geo IP information.

Syntax

```
diagnose system geoip info
diagnose system geoip dump
diagnose system geoip <ip>
```

Variable	Description
info	Display brief geo IP information.
dump	Display all geo IP information.
<ip>	Find the IP address' country.

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

Variable	Description
status	List NTP servers' information.

Example

This is an example of the output from diagnose system ntp status:

```
server ntp1.fortinet.net (208.91.112.50) -- Clock is synchronized
server-version=4, stratum=2
reference time is d4a03db3.52abe82f -- UTC Tue Jan 15 20:42:27 2013
clock offset is 0.210216 msec, root delay is 1649 msec
root dispersion is 2075 msec, peer dispersion is 2 msec
```

system print

Use this command to print server information.

Syntax

```
diagnose system print certificate
diagnose system print cpuinfo
diagnose system print df
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
```

```
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

Variable	Description
certificate	Print the IPsec certificate.
cpuinfo	Print the CPU information. This command includes the following: processor, vendor ID, CPU family, model, model name, stepping, CPU MHz, cache size, physical ID, sibling,
df	Print the file system disk space usage. This command displays the following information: file system, 1K-blocks, used, available, percent used, mounted on.
hosts	Print the static table lookup for host names.
interface <interface>	Print the information of the interface. This command displays the following information: status, speed, duplex, supported ports, auto-negotiation, advertised link modes, and advertised auto-negotiation.
loadavg	Print the average load of the system.
netstat	Print the network statistics for active Internet connections (servers and established). This command displays the following information: protocol, local address, foreign address, and state.
partitions	Print the partition information of the system.
route	Print the main route list. This command displays the following information: destination, gateway, gateway mask, flags, metric, reference, use, and interface,
rtcache	Print the contents of the routing cache.
slabinfo	Print the slab allocator statistics.
sockets	Print the currently used socket ports. This command displays the following information: number, protocol, and port.
uptime	Print how long the system has been running.

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process kill -<signal> <pid>
diagnose system process killall <module>
diagnose system process list
```

Variable	Description
`kill -<signal> <pid>`	Kill a process. For example: -9 or -KILL
`killall <module>`	Kill all the related processes.
`list`	List all processes running on the FortiAnalyzer. This command displays the PID, UID, stat, and command.

system raid

Use this command to view RAID information.

Syntax

```
diagnose system raid alarms
diagnose system raid hwinfo
diagnose system raid status
```

Variable	Description
`alarms`	Show RAID alarm logs.
`hwinfo`	Show RAID controller hardware information.
`status`	Show RAID status. This command displays the following information: RAID level, RAID status, RAID size, and hard disk information.

system route

Use this command to diagnose routes.

Syntax

```
diagnose system route list
```

Variable	Description
`list`	List all routes. This command displays the following information: destination IP, gateway IP, netmask, flags, metric, reference, use, and interface.

system route6

Use this command to diagnose IPv6 routes.

Syntax

```
diagnose system route6 list
```

Variable	Description
`list`	List all IPv6 routes. This command displays the following information: destination IP, gateway IP, interface, metric, and priority.

test

Use the following commands to test the FortiAnalyzer:

- test application
- test connection
- test sftp

test application

Use this command to test application daemons. Leave the integer value blank to see the available options for each command.

Syntax

```
diagnose test application fazautormd <integer>
diagnose test application fazcfgd <integer>
diagnose test application fazsvcd <integer>
diagnose test application fortilogd <integer>
diagnose test application logfiled <integer>
diagnose test application oftpd <integer>
diagnose test application snmpd <integer>
diagnose test application sqllogd <integer>
diagnose test application sqlrptcached <integer>
```

Variable	Description
`fazautormd <integer>`	Test the FortiAnalyzer automatic delete daemon.
`fazcfgd <integer>`	Test the FortiAnalyzer configuration daemon.
`fazsvcd <integer>`	Test the FortiAnalyzer service daemon.
`fortilogd <integer>`	Test the FortiAnalyzer `fortilogd` daemon.

Variable	Description
logfiled <integer>	Test the FortiAnalyzer log file daemon.
oftpd <integer>	Test the FortiAnalyzer oftpd daemon.
snmpd <integer>	Test the SNMP daemon.
sqllogd <integer>	Test the FortiAnalyzer sqllog daemon.
sqlrptcached <integer>	Test the FortiAnalyzer sqlrptcache daemon.

test connection

Test the connection to the mail server and syslog server.

Syntax

```
diagnose test connection mailserver <server-name> <account>
diagnose test connection syslogserver <server-name>
```

Variable	Description
<server-name>	The name of the SMTP server.
<account>	Enter an email account to which a test email will be sent to.

test sftp

Use this command to test the secure file transfer protocol (SFTP).

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

Variable	Description	Default
<sftp server>	SFTP server IP address.	
<username>	SFTP server username.	
<password>	SFTP server password.	
<directory>	The directory variable represents the directory on the SFTP server where you want to put the file.	"/"

upload

Use the following commands for upload related settings.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear all
diagnose upload clear failed
```

Variable	Description
`all`	Clear all upload requests.
`failed`	Clear the failed upload requests.

upload force-retry

Use this command to retry the last failed upload request.

Syntax

```
diagnose upload force-retry
```

upload status

Use this command to get the running status on files in the upload queue.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD
diagnose vpn tunnel list
```

Variable	Description
`flush-SAD`	Flush the SAD entries.
`list`	List tunnel information.

get

The `get` commands display a part of your FortiAnalyzer unit's configuration in the form of a list of settings and their values.

Although not explicitly shown in this section, for all `config` commands there are related get and show commands that display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise specified.

FortiAnalyzer commands and variables are case sensitive.

The get command displays all settings, even if they are still in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

This chapter contains following sections:

system admin
system aggregation-client
system aggregation-service
system alert-console
system alert-event
system alertemail
system auto-delete
system backup
system certificate
system dns
system fips
system global
system interface
system locallog
system log
system mail
system ntp
system password-policy
system performance
system report
system route
system route6
system snmp
system sql
system status
system syslog

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group <group name>
get system admin ldap <server entry name>
get system admin profile <profile ID>
get system admin radius <server entry name>
get system admin setting
get system admin tacacs <server entry name>
get system admin user <username>
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin_server_cert : server.crt
allow_register : disable
auto-update : enable
banner-message : (null)
chassis-mgmt : disable
chassis-update-interval : 15
demo-mode : disable
device_sync_status : enable
http_port : 80
https_port : 443
idle_timeout : 480
install-ifpolicy-only : disable
mgmt-addr : (null)
mgmt-fqdn : (null)
offline_mode : disable
register_passwd : *
show-add-multiple : enable
show-adom-central-nat-policies : disable
show-adom-devman : enable
show-adom-dos-policies : disable
show-adom-dynamic-objects : enable
show-adom-icap-policies : enable
show-adom-implicit-policy : enable
show-adom-ipv6-settings : enable
show-adom-policy-consistency-button : disable
show-adom-rtmlog : disable
show-adom-sniffer-policies : disable
show-adom-taskmon-button : enable
show-adom-terminal-button : disable
show-adom-voip-policies : enable
show-adom-vpnman : enable
show-adom-web-portal : disable
show-device-import-export : enable
show-foc-settings : enable
show-fortimail-settings : disable
show-fsw-settings : enable
show-global-object-settings : enable
show-global-policy-settings : enable
show_automatic_script : disable
show_grouping_script : disable
show_tcl_script : disable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system aggregation-client

Use this command to view log aggregation settings.

Syntax

```
get system aggregation-client <id>
```

Example

This example shows the output for `get system aggregation-client`:

```
id : 1
mode : realtime
fwd-facility : local7
fwd-log-source-ip : local_ip
fwd-min-level : information
fwd-remote-server : fortianalyzer
server-ip : 1.1.11.1
```

system aggregation-service

Use this command to view log aggregation service settings.

Syntax

```
get system aggregation-service
```

Example

This example shows the output for `get system aggregation-service`:

```
accept-aggregation : enable
aggregation-disk-quota: 1234
password : *
```

system alert-console

Use this command to view the alert console settings.

Syntax

```
get system alert-console
```

Example

This example shows the output for `get system alert-console`:

```
period : 7
severity-level : information
```

system alert-event

Use this command to view alert event settings.

Syntax

```
get system alert-event <alert name>
```

Example

This example shows the output for `get system alert-event Test`:

```
name : Test
alert-destination:
== 1 ==
enable-generic-text : enable
enable-severity-filter: enable
event-time-period : 0.5
generic-text : Test
num-events : 1
severity-filter : medium-low
severity-level-comp : =
severity-level-logs : information
```

system alertemail

Use this command to view alertemail settings.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, archived and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
Last Backup: Tue Jan 15 16:55:35 2013
Next Backup: N/A
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca <certificate name>
get system certificate crl <crl name>
get system certificate local <certificate name>
get system certificate oftp <certificate name>
get system certificate ssh <certificate name>
```

Example

This example shows the output for `get system certificate CA Fortinet_CA`:

```
name : Fortinet_CA
ca :
   Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
       Authority, CN = support, emailAddress = support@fortinet.com
   Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
       Authority, CN = support, emailAddress = support@fortinet.com
   Valid from: 2000-04-09 01:25:49 GMT
   Valid to: 2038-01-19 03:14:07 GMT
   Fingerprint:
   Root CA: Yes
   Version: 3
   Serial Num:
      00
   Extensions:
      Name: X509v3 Basic Constraints
      Critical: no
      Content:
      CA:TRUE
comment : Default CA certificate
```

system dns

Use this command to view DNS settings.

Syntax

```
get system dns
```

Example

This example shows the output for `get system dns`:

```
primary : 208.91.112.53
secondary : 208.91.112.63
```

system fips

Use this command to view FIPS settings.

Syntax

```
get system fips
```

Example

This example shows the output for `get system fips`:

```
fortitrng : enable
re-seed-interval : 1440
```

system global

Use this command to view global system settings.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-https-pki-required: disable
admin-lockout-duration: 60
admin-lockout-threshold: 3
admin-maintainer : enable
admintimeout : 5
adom-mode : advanced
adom-status : enable
auto-register-device: enable
backup-compression : normal
```

```
backup-to-subfolders: disable
clt-cert-req : disable
console-output : standard
daylightsavetime : enable
default-disk-quota : 1000
enc-algorithm : low
hostname : FortiAnalyzer-2000B
language : english
ldapconntimeout : 60000
log-checksum : md5-auth
log-mode : analyzer
max-concurrent-users: 20
max-running-reports : 1
pre-login-banner : disable
remoteauthtimeout : 10
ssl-low-encryption : enable
swapmem : enable
timezone : (GMT-8:00) Pacific Time (US & Canada).
webservice-support-sslv3: disable
```

system interface

Use these commands to view interface configuration and status.

Syntax

```
get system interface
get system interface <interface name>
```

Examples

This example shows the output for `get system interface`:

```
name Interface name.
port1 up 172.16.81.60 255.255.255.0 auto
port2 up 192.168.2.99 255.255.255.0 auto
port3 up 192.168.3.99 255.255.255.0 auto
port4 up 192.168.4.99 255.255.255.0 auto
port5 up 192.168.5.99 255.255.255.0 auto
port6 up 192.168.6.99 255.255.255.0 auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : up
ip : 172.16.81.60 255.255.255.0
allowaccess : ping https ssh telnet http webservice aggregator
serviceaccess :
speed : auto
description : (null)
alias : (null)
ipv6:
ip6-address: ::/0 ip6-allowaccess:
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
get system locallog fortianalyzer filter
get system locallog fortianalyzer setting
get system locallog memory filter
get system locallog memory setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Examples

This example shows the output for `get system locallog disk filter`:

```
event : enable
dvm : enable
fmgws : disable
iolog : enable
system : enable
```

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : notification
upload : disable
server-type : FTP
max-log-file-size : 100
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
```

system log

Use these commands to view log settings:

Syntax

```
get system log alert
get system log fortianalyzer
get system log settings
```

Example

This example shows the output for `get system log fortianalyzer`:

```
status : disable
ip : 0.0.0.0
secure_connection : disable
username : admin
passwd : *
```

```
auto_install : disable
```

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail <server name>
```

Example

This example shows the output for `get system mail Test2`:

```
server : Test2
auth : enable
passwd : *
port : 25
user : test@fortinet.com
```

system ntp

Use this command to view NTP settings.

Syntax

```
get system ntp
```

Example

This example shows the output for `get system ntp`:

```
ntpserver:
== [ 1 ]
id: 1
status : enable
sync_interval : 60
```

system password-policy

Use this command to view the system password policy.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
```

```
minimum-length : 8
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 60
```

system performance

Use this command to view performance statistics on your FortiAnalyzer unit.

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
Used: 2.7%
Used(Excluded NICE): 2.6%
CPU_num: 4.
CPU[0] usage: 5%
CPU[1] usage: 3%
CPU[2] usage: 0%
CPU[3] usage: 3%
Memory:
Total: 5,157,428 KB
Used: 666,916 KB 12.9%
Hard Disk:
Total: 4,804,530,144 KB
Used: 3,260,072 KB 0.1%
Flash Disk:
Total: 38,733 KB
Used: 37,398 KB 96.6%
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report setting
```

Example

This example shows the output for `get system report auto-cache`:

```
aggressive-drilldown : disable
drilldown-interval : 168
status : enable
```

system route

Use this command to view routing table configuration.

Syntax

```
get system route <seq_num>
```

Example

This example shows the output for `get system route 1`:

```
seq_num : 1
device : port1
dst : 0.0.0.0 0.0.0.0
gateway : 172.16.81.1
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 <entry number>
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community <community ID>
get system snmp sysinfo
get system snmp user <SNMP user name>
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description : (null)
engine-id : (null)
location : (null)
status : disable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system sql

Use this command to view SQL settings.

Syntax

```
get system sql
```

system status

Use this command to view the status of your FortiAnalyzer unit.

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```
Platform Type : FAZ4000B
Platform Full Name : FortiAnalyzer-4000B
Version : v5.2.0-build0574 140606 (Interim)
Serial Number : FL-4KB3M10600006
BIOS version : 00010016
Hostname : FAZ4000B
Max Number of Admin Domains : 2000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 574
Release Version Information : Interim
Current Time : Wed Jun 11 13:49:39 PDT 2014
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
64-bit Applications : Yes
Disk Usage : Free 9155.59GB, Total 9157.91GB
```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog <name of syslog server>
```

show

The `show` commands display a part of your Fortinet unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.

FortiAnalyzer commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are assumed to remain in their default state.

The following examples show the difference between the output of the show command branch and the get command branch.

Example show command

```
show system dns
config system dns
   set primary 208.91.112.53
   set secondary 208.91.112.63
end
```

Example get command

```
get system dns
primary : 208.91.112.53
secondary : 208.91.112.63
```

Appendix A - Object Tables

Global object categories

38 "webfilter ftgd-local-cat"	47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"
52 "vpn certificate ca"	56 "spamfilter bword"	60 "spamfilter dnsbl"
64 "spamfilter mheader"	67 "spamfilter iptrust"	85 "ips custom"
140 "firewall address"	142 "firewall addrgrp"	255 "user adgrp"
145 "user radius"	146 "user ldap"	147 "user local"
148 "user peer"	152 "user group"	167 "firewall service custom"
254 "firewall service predefined"	168 "firewall service group"	170 "firewall schedule onetime"
171 "firewall schedule recurring"	172 "firewall ippool"	173 "firewall vip"
288 "ips sensor"	292 "log custom-field"	293 "user tacacs+"
296 "firewall ldb-monitor"	1028 "application list"	1038 "dlp sensor"
1043 "wanopt peer"	1044 "wanopt auth-group"	1054 "vpn ssl web portal"
1076 "system replacemsg-group"	1097 "firewall mms-profile"	1203 "firewall gtp"
1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1327 "webfilter content"
1337 "endpoint-control profile"	1338 "firewall schedule group"	1364 "firewall shaper traffic-shaper"
1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"	1370 "vpn ssl web host-check-software"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1472 "antivirus mms-checksum"	1482 "voip profile"	150 "system object-tag"
184 "user fortitoken"	273 "web-proxy forward-server"	335 "dlp filepattern"
343 "icap server"	344 "icap profile"	321 "user fsso"

390 "system sms-server"	397 "spamfilter bwl"	457 "wanopt profile"
384 "firewall service category"	474 "application custom"	475 "user device-category"
476 "user device"	492 "firewall deep-inspection-options"	800 "dynamic interface"
810 "dynamic address"	1004 "vpnmgr vpntable"	1005 "vpnmgr node"
1100 "system meta"	820 "report output"	822 "sql-report chart"
824 "sql-report dataset"	825 "sql-report dashboard"	827 "sql-report layout"
1494 "dynamic vip"	1495 "dynamic ippool"	1504 "dynamic certificate local"
1509 "dynamic vpntunnel"		

Device object ID values

1 "system vdom"	3 "system accprofile"	5 "system admin"
8 "system interface"	16 "system replacemsg mail"	17 "system replacemsg http"
18 "system replacemsg ftp"	19 "system replacemsg nntp"	20 "system replacemsg alertmail"
21 "system replacemsg fortiguard-wf"	22 "system replacemsg spam"	23 "system replacemsg admin"
24 "system replacemsg auth"	25 "system replacemsg im"	26 "system replacemsg sslvpn"
28 "system snmp community"	38 "webfilter ftgd-local-cat"	1300 "application recognition predefined"
47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"	52 "vpn certificate ca"
53 "vpn certificate local"	54 "vpn certificate crl"	55 "vpn certificate remote"
56 "spamfilter bword"	60 "spamfilter dnsbl"	64 "spamfilter mheader"
67 "spamfilter iptrust"	74 "imp2p aim-user"	75 "imp2p icq-user"
76 "imp2p msn-user"	77 "imp2p yahoo-user"	85 "ips custom"
117 "system session-helper"	118 "system tos-based-priority"	124 "antivirus service"
128 "antivirus quarfilepattern"	130 "system ipv6-tunnel"	314 "system sit-tunnel"

131 "system gre-tunnel"	132 "system arp-table"	135 "system dhcp server"
137 "system dhcp reserved-address"	138 "system zone"	140 "firewall address"
142 "firewall addrgrp"	255 "user adgrp"	145 "user radius"
146 "user ldap"	147 "user local"	148 "user peer"
152 "user group"	155 "vpn ipsec phase1"	156 "vpn ipsec phase2"
157 "vpn ipsec manualkey"	158 "vpn ipsec concentrator"	165 "vpn ipsec forticlient"
167 "firewall service custom"	254 "firewall service predefined"	168 "firewall service group"
170 "firewall schedule onetime"	171 "firewall schedule recurring"	172 "firewall ippool"
173 "firewall vip"	178 "firewall ipmacbinding table"	181 "firewall policy"
189 "firewall dnstranslation"	190 "firewall multicast-policy"	199 "system mac-address-table"
200 "router access-list"	202 "router aspath-list"	204 "router prefix-list"
206 "router key-chain"	208 "router community-list"	210 "router route-map"
225 "router static"	226 "router policy"	253 "system proxy-arp"
284 "system switch-interface"	285 "system session-sync"	288 "ips sensor"
292 "log custom-field"	293 "user tacacs+"	296 "firewall ldb-monitor"
297 "ips decoder"	299 "ips rule"	307 "router auth-path"
317 "system wccp"	318 "firewall interface-policy"	1020 "system replacemsg ec"
1021 "system replacemsg nac-quar"	1022 "system snmp user"	1027 "application name"
1028 "application list"	1038 "dlp sensor"	1041 "user ban"
1043 "wanopt peer"	1044 "wanopt auth-group"	1045 "wanopt ssl-server"
1047 "wanopt storage"	1054 "vpn ssl web portal"	1061 "system wireless ap-status"
1075 "system replacemsg-image"	1076 "system replacemsg-group"	1092 "system replacemsg mms"
1093 "system replacemsg mm1"	1094 "system replacemsg mm3"	1095 "system replacemsg mm4"
1096 "system replacemsg mm7"	1097 "firewall mms-profile"	1203 "firewall gtp"

1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1326 "system replacemsg traffic-quota"
1327 "webfilter content"	1337 "endpoint-control profile"	1338 "firewall schedule group"
1364 "firewall shaper traffic-shaper"	1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"
1370 "vpn ssl web host-check-software"	1373 "report dataset"	1375 "report chart"
1382 "report summary"	1387 "firewall sniff-interface-policy"	1396 "wireless-controller vap"
1399 "wireless-controller wtp"	1402 "wireless-controller ap-status"	1412 "system replacemsg web-proxy"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1440 "firewall profile-protocol-options"	1453 "firewall profile-group"	1461 "system storage"
1462 "report style"	1463 "report layout"	1472 "antivirus mms-checksum"
1482 "voip profile"	1485 "netscan assets"	1487 "firewall central-nat"
1490 "report theme"	150 "system object-tag"	169 "system dhcp6 server"
180 "system port-pair"	182 "system 3g-modem custom"	183 "application rule-settings"
184 "user fortitoken"	212 "webfilter override"	270 "firewall local-in-policy"
273 "web-proxy forward-server"	330 "system ddns"	331 "system replacemsg captive-portal-dflt"
335 "dlp filepattern"	337 "dlp fp-sensitivity"	338 "dlp fp-doc-source"
342 "webfilter ftgd-warning"	343 "icap server"	344 "icap profile"
352 "system monitors"	354 "system sp"	321 "user fsso"
355 "router gwdetect"	386 "system physical-switch"	388 "system virtual-switch"
390 "system sms-server"	394 "system replacemsg utm"	397 "spamfilter bwl"
406 "vpn certificate ocsp-server"	408 "user password-policy"	412 "webfilter search-engine"
428 "firewall identity-based-route"	431 "web-proxy debug-url"	432 "firewall ttl-policy"
434 "firewall isf-acl"	435 "firewall DoS-policy"	437 "firewall sniffer"

438 "wireless-controller wids-profile"	439 "switch-controller vlan"	441 "switch-controller managed-switch"
453 "firewall ip-translation"	457 "wanopt profile"	269 "firewall multicast-address"
384 "firewall service category"	466 "system ips-urlfilter-dns"	467 "system geoip-override"
474 "application custom"	475 "user device-category"	476 "user device"
483 "system server-probe"	473 "system replacemsg device-detection-portal"	492 "firewall deep-inspection-options"

Appendix B - Maximum Values Table

Maximum values tables

Feature	FAZ-100C, 200D	FAZ-300D, 400B, 400C	FAZ-1000B, 1000C, 1000D	FAZ-2000A, 2000B	FAZ-3000D, 3000E, 4000A, 4000B	FAZ-3500E, 3900E,
Administrative Domains (ADOMS)	100, 150	175, 200, 300	2000	2000	2000	4000
Administrators	256	256	256	256	256	256
Administrator access profiles	256	256	256	256	256	256
SNMP community	256	256	256	256	256	256
SNMP managers per community	256	256	256	256	256	256
Email servers	256	256	256	256	256	256
Syslog servers	256	256	256	256	256	256
TACACS+ servers	256	256	256	256	256	256
Administrator RADIUS servers	256	256	256	256	256	256
Administrator LDAP servers	256	256	256	256	256	256
Static routes	256	256	256	256	256	256
NTP Servers	256	256	256	256	256	256
Log devices	100, 150	175, 200, 300	2000	2000	2000	4000
Devices per ADOM	100, 150	175, 200, 300	2000	2000	2000	4000
Report output profiles	250	250	500	750	1000	1000

Feature	FAZ-100C, 200D	FAZ-300D, 400B, 400C	FAZ-1000B, 1000C, 1000D	FAZ-2000A, 2000B	FAZ-3000D, 3000E, 4000A, 4000B	FAZ-3500E, 3900E,
SQL report templates	1000	1000	1000	1000	1000	1000
SQL report charts	1000	1000	1000	1000	1000	1000
SQL report datasets	1000	1000	1000	1000	1000	1000
SQL database size (GB)	1000	4000, 1000,2000	1000, 8000	3K, 12K	16K, 6K, 24K	

Feature	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Administrative Domains (ADOMS)	10000	10000	10000	10000	10000
Administrators	256	256	256	256	256
Administrator access profiles	256	256	256	256	256
SNMP community	256	256	256	256	256
SNMP managers per community	256	256	256	256	256
Email servers	256	256	256	256	256
Syslog servers	256	256	256	256	256
TACACS+ servers	256	256	256	256	256
Administrator RADIUS servers	256	256	256	256	256
Administrator LDAP servers	256	256	256	256	256
Static routes	256	256	256	256	256
NTP Servers	256	256	256	256	256
Log devices	10000	10000	10000	10000	10000
Devices per ADOM	10000	10000	10000	10000	10000

Feature	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Report output profiles	1000	1000	1000	1000	1000
SQL report templates	1000	1000	1000	1000	1000
SQL report charts	1000	1000	1000	1000	1000
SQL report datasets	1000	1000	1000	1000	1000
SQL database size (GB)	200	+200	+1000	+8K	+16K

Appendix C - CLI Error Codes

Some FortiAnalyzer CLI commands issue numerical error codes. The following table lists the error codes and descriptions.

Error Code	Description
0	Success
1	Function called with illegal parameters
2	Unknown protocol
3	Failed to connect host
4	Memory failure
5	Session failure
6	Authentication failure
7	Generic file transfer failure
8	Failed to access local file
9	Failed to access remote file
10	Failed to read local file
11	Failed to write local file
12	Failed to read remote file
13	Failed to write remote file
14	Local directory failure
15	Remote directory failure

FORTINET®

High Performance Network Security

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.